Guía de Hacking del Neófito

Por ~deicide

Edición 1.2

Completada el 28/8/1993

Modificación 1.1 Terminada el 10/10/93

Modificación 1.2 Terminada el 10/23/93

El autor de este fichero otorga permiso para reproducir y redistribuir el mismo de cualquier manera que el lector lo considere, incluyendo la inclusión de este fichero en boletines de cualquier tipo, provisto que este fichero se mantenga entero y completo, sin modificación alguna, omisiones o eliminaciones

(c) 1993, Deicide

Tabla de Contenidos

1. INTRODUCCIÓN

2. ÉTICA/SEGURIDAD

3. DONDE COMENZAR

4. REDES DE CONMUTACIÓN DE PAQUETES

    A. Introducción al PSNs

    B. Cómo funcionan las conmutación de paquetes

    C. La Internet

        1. Introducción

        2. Logrando Acceso

        3. FTP

    D. Redes X.25

        1. NUAs

        2. PADs & NUIs

        3. CUGs

        4. SprintNet

        5. BT Tymnet

        6. Datapac

        7. DNIC List

5. PENETRACIÓN DE SISTEMAS

    A. Unix

    B. VMS

    C. MPE (mainframes HP3000)

    D. VM/CMS

    E. Primos

    F. TOPS 10/20

    G. IRIS

    H. NOS

    I. DEC Server

J. GS/1

K. XMUX

L. Starmaster/PACX

M. Access 2590

N. PICK

O. AOS/VS

P. RSTS

Q. WindowsNT

R. Novell Netware

S. System75/85

T. AS400

U. TSO

6. FUERZA BRUTA

A. Contraseñas

B. Nombres de Usuario

C. Servicios

7. INGENIERÍA SOCIAL

8. REGISTRO DE BASURA

9. ACRÓNIMOS

10. CONCLUSIÓN

A. Palabras Finales

B. Lectura Recomendada

C. BBSes

D. Referencias

E. Y finalmente..

F. Aviso Legal

Introducción

Han pasado más de cuatro años desde la creación y distribución de la versión final de la *Guía del Novicio al Hacking* por parte de la LOD/H *[N.de.T: Legión del Terror/Legión de Hackers, supergrupo de hacking estadounidense principalmente activo desde 1984 a 1991]* sobre la temática hacking. Desde entonces esta ha servido como valiosa fuente de conocimiento para muchos hackers que comienzan a explorar las maravillas de la penetración y exploración de sistemas.

La guía ha demostrado ser muy necesaria para una parva de novatos que sin tener ni idea de lo que era una VAX, estaban ansiosos por aprender el arcano arte del hacking. Muchos de los hackers más experimentados y moderados de la actualidad han recurrido a la guía como valiosa referencia durante sus primeros pasos tentativos (o no) en el ciberespacio.

Sin embargo, el paso del tiempo ha afectado a las redes informáticas y dicha guía se encuentra ahora algo desactualizada. Las configuraciones predeterminadas básicas de los fabricantes suelen estar protegidas, y han surgido nuevos sistemas operativos que ocupan una gran parte del mercado. En más de cuatro años, no se ha hecho ni un solo intento decente de redactar una secuela, por razones que desconozco.

De manera tal que decidí poner manos a la obra y crear mi propia guía de hacking: la "Guía de Hacking del Neófito" (¡no se rían!), con la esperanza de que pueda ayudar a otros a profundizar en sus exploraciones de la red. Esta guía se basa en la original, principalmente porque la original *era* buena. Se han añadido nuevas secciones y se han ampliado las antiguas. Sin embargo, no constituye esta una simple actualización, sino mas bien una apuesta de guía completamente nueva, como apreciarán por la diferencia de tamaño. Esta guía resultó ser más de cuatro veces más grande que la guía de The Mentor.

Además, esta guía NO es una "secuela" real de la original; no está patrocinada ni autorizada por la LOD/H, ni nada por el estilo, principalmente porque la LOD/H ya no existe. Una última cosa... esta guía no es exhaustiva. Hay muchos sistemas operativos que no he incluido, principalmente por su rareza o mi falta de experiencia con ellos. Cubro los principales sistemas operativos, pero en futuras versiones me gustaría tratar Wang, MVS, CICS, SimVTAM, Qinter, IMS, VOS y muchos más. Si crees que puedes serme de ayuda al respecto, por favor contáctame a través del correo electrónico, en una BBS o en Internet (si logras encontrarme). Lo mismo aplica en lo que refiere a la ampliación de los temas tratados y sistemas operativos actuales; por favor, contáctame.

Está bien, ya ha sido una introducción bastante larga, pero bueno... disfrútala.

Deicide - deicide@west.darkside.com

Ética/Seguridad

Uno de los aspectos más importantes de la mentalidad de un hacker es su código ético. Y la ética suele ir de la mano con la seguridad, que – obviamente si planeas vivir fuera de la cárcel - es la parte más crítica del proceso de hackeo y exploración de sistemas.

La ética de un hacker suele ser algo diferente a la de un tipo común. A un tipo común se le enseña que está mal infringir las leyes, aunque la mayoría lo hace de todos modos. Yo particularmente te animo a que infrinjas las leyes, pero en busca de conocimiento. En mi opinión, si el hackeo se realiza con las intenciones correctas, no es tan criminal. Los medios de comunicación nos hacen parecer sociópatas psicópatas empeñados en provocar el apocalipsis con nuestras computadoras. Es poco probable. Probablemente podría darle la vuelta a la tortilla a los medios alarmistas demostrando que un evasor impositivo típico perjudica más al sistema que un intruso curioso, pero me abstengo... que se regodeen...

Lo que un hacker nunca debe hacer es hackear maliciosamente un sistema (también conocido como bloquear, dañar, *crashear*, *trashear*, etc.). Borrar y modificar archivos innecesariamente es MALO. No sirve para nada más que para que los administradores del sistema te busquen para matarte y te quiten la cuenta. Patético. No lo hagas.

En fin, si no entiendes todo esto, haz lo posible por seguirlo y confía en mi palabra. Entenderás el razonamiento detrás de estas pautas más adelante.

I. Nunca hackees maliciosamente un sistema. No borres ni modifiques archivos innecesariamente, ni ralentices o bloquees un sistema de manera intencionada. La única excepción a esta regla es la modificación de los registros de auditoría del sistema y para ocultar tus rastros de tus huellas.

II. No des tu nombre ni tu número de teléfono real a NADIE, no importa quién sea. Algunos de los hackers más famosos se han convertido en informantes porque han sido descubiertos, y te delatarán si les das la oportunidad. Se dice que uno de cada tres hackers es un agente federal, y aunque esto es una exageración, considéralo una regla y no tendrás problemas. Reúnete con ellos en un bucle telefónico, alianza, cartelera electrónica, sistema de chat, lo que sea, pero no des tu número de telefónico.

III. Mantente alejado de las computadoras del gobierno. Descubrirás muy pronto que intentar hackear una instalación militar es prácticamente imposible y te arrestarán antes de que puedas decir "¡mierda!". El Gran Hermano tiene recursos infinitos y todo el tiempo que necesita para darte caza: pasarán años buscándote. Por muy tentador que sea, no te precipites, te arrepentirás al final.

IV. ¡Nunca uses c0dez desde tu propia casa! Punto. Esto es lo más increíblemente patético que he visto en mi vida en el mundo clandestino; un abuso increíble de c0dez, que ha sido la perdición de muchísimas personas. La mayoría de las PBX/950/800 cuentan con ANI, y usarlos te llevará a la atrapada, sin duda. Y las tarjetas telefónicas prepagas son una idea incluso peor. Los c0dez son una forma de pseudo-phreaking que no tiene nada que ver con la exploración de las redes telefónicas, que es de lo que trata el phreaking. Si eres demasiado perezoso para practicar el phreaking o ser ingenioso, entonces olvídate del phreaking.

V. No incrimines a otros, por mucho que los odies. Denunciar a otros hackers por una disputa es una pésima manera de resolver las cosas; Dales una paliza, córtales el teléfono/la luz/el agua, lo que sea, pero no los delates. Al final, se te volverá en contra.

VI. Ten cuidado con lo que publicas. Como regla general, no publiques cuentas ni códigos en redes abiertas. Morirán en cuestión de días y perderás tu nuevo tesoro. Publicar números de tarjetas de crédito es un delito penal, según una ley aprobada durante la era Reagan.

VII. No compres artículos con tarjeta ajena. Esto es incluso peor que usar c0dez; las probabilidades de que te atrapen son muy altas.

VIII. Si por alguna razón tienes que usar c0dez, usa los tuyos y nada más. Nunca uses un c0de que veas en una cartelera electrónica, porque lo más probable es que ya haya sido usado indebidamente, y por lo tanto esté siendo monitoreado.

IX. Siéntete libre de hacer preguntas, pero con sensatez. Los hackers no siempre estarán dispuestos a compartir datos de irrupción a cuentas, y si este es el caso, no te sorprendas. Como regla general, formula preguntas técnicas. Intenta aprender todo lo que puedas mediante la experiencia práctica.

X. Y, por último, sé precavido. Emplea PGP para cifrar tus ficheros, guarda tus notas/volcados de impresión en un lugar secreto y seguro, haz lo que sea necesario para prolongar tu estancia fuera del mundo de la telefonía móvil.

XI. Si te pillan, no digas NADA a las autoridades. Niégate a hablar con ellas sin la presencia de un abogado.

XII. Si la policía llega a tu domicilio para ejecutar una orden de allanamiento, revísala cuidadosamente; es tu derecho. Averigua qué pueden y qué no pueden hacer, y si no pueden hacer algo, asegúrate de que no lo hagan.

XIII. Si es posible, Intenta no hackear tu propia línea telefónica. Empalma la línea de tu vecino, llama desde un Fortress Fone, hackea una caja de conexiones, lo que sea... si hackeas durante el tiempo suficiente, es probable que algún día te rastreen o te registren en la base de datos ANI. Tampoco creas que estás completamente a salvo en redes de conmutación de paquetes, lleva tiempo, pero si escaneas/hackeas tu punto de acceso local, lo rastrearán.

XIV. Dificulta al máximo el rastreo para los demás. Rebota la llamada en varios números de marcación saliente (*outdials*) o intenta pasar por al menos dos compañías telefónicas diferentes al discar a un nodo de acceso telefónico. Cuando estés en una red de conmutación de paquetes o en una red de área local o amplia, intenta rebotar la llamada en varios PADs o a través de otras redes antes de arribar a tu corresponsal de destino. Cuantos más rebotes, más papeleo para el investigador y más fácil te será escapar sin dejar rastro. Intenta no permanecer demasiado tiempo en ningún sistema y alterna tus horas y fechas de discado.

XV. ¡No guardes notas escritas! Mantén toda la información en la computadora, cifrada con PGP u otro programa de cifrado de estándar militar. Las notas escritas solo te incriminarán en un tribunal. Si escribes algo originalmente, tritura el papel... en

pedacitos pequeños es mejor, o mejor aún, ¡quémalo! Los federales también registran los residuos, igual que nosotros, y si tiras tus notas completas, terminarán en sus manos y las usarán en tu contra.

XVI. Finalmente está la controversia de las llamadas diurnas/nocturnas... Algunos piensan que es mejor llamar durante el día (o cuando el usuario normalmente use su cuenta) para no despertar las sospechas del administrador del sistema sobre horarios de llamada anormales, mientras que otros piensan que es mejor llamar cuando no haya nadie.

Este es un tema complejo, ya que no hay una respuesta definitiva. Si el administrador del sistema guarda registros (y los revisa), sin duda le parecerá extraño que una secretaria disque el módem a las 3 de la mañana. Probablemente, después de investigar más a fondo, encontrará aún más extraño que la secretaria haya descargado el fichero de contraseñas y procedido a configurar entrada de una consola de root. Por otro lado, si llamas durante el horario habitual del usuario, el verdadero propietario legítimo de la cuenta podría iniciar sesión y ver su nombre ya registrado, o peor aún, que se le deniegue el acceso porque su cuenta se encuentra en uso en ese preciso instante.

Al final, todo depende de tu opinión. Y recuerda, cuando tomes una decisión, mantente firme; recuerda que la zona horaria cambia.

¿Por dónde comenzar?

Probablemente, la etapa más difícil en el hacking sea la de los primeros pasos.

Encontrar y penetrar tu primer sistema es un paso fundamental, y se puede abordar de muchas maneras. Las formas más comunes de encontrar un sistema para hackear son:

- UNIVERSIDADES: Las universidades suelen contar con cientos de estudiantes, muchos de los cuales no tienen mucha experiencia en informática, lo que hace que hackear sea una tarea relativamente sencilla. Además, la seguridad suele ser deficiente, así que si no abusas demasiado del sistema, tu estancia podría ser larga.
  Por otro lado, por una pequeña tarifa, normalmente puedes conseguir una cuenta barata *legítima* (¡menudo concepto!).
  O podrías matricularte en la universidad para obtener algunos créditos y seguir hasta que se acaben las cuentas. Desafortunadamente, si te pillan hackeando tu propia cuenta, no será difícil rastrearla hasta ti. Si al principio consigues una cuenta legítima, quizás lo mejor sea hackear la cuenta de otro estudiante para hackear otros sistemas.
  Otra ventaja de las universidades es que a menudo proporcionan acceso a varias redes, generalmente incluyendo Internet. Ocasionalmente también tendrás acceso a PSN.
- ESCANEO DE OPERADORES (WARDIALING): El escaneo de operadores en tu LATA (Área de Transporte de Acceso Local), conocida comúnmente como wardialing, se popularizó en la película Juegos de Guerra.
  Desafortunadamente, existen algunos problemas inherentes a encontrar sistemas de esta manera; estás limitado a los sistemas de tu área, por lo que si vives en un pueblo pequeño, puede que encuentres muy poco de interés; y, en segundo lugar, el ANI es un problema dentro de tu propia LATA, y el rastreo es sencillo, lo que aumenta los riesgos de seguridad. Si vas a hackear un sistema dentro de tu propia red local, haz un rebotado al menos una vez. Existen muchos programas, como ToneLoc y CodeThief (ToneLoc es superior a todos en mi humilde opinión), que automatizan este proceso.
- CONMUTACIÓN DE PAQUETES: Este es mi favorito con diferencia, ya que hackear en PSN es como Aprendí casi todo lo que sé. He explorado PSN en todo el mundo y nunca me he quedado sin sistemas para hackear. No importa qué PSN pruebes, encontrarás muchos sistemas diferentes que se pueden hackear. Profundizaré más en las PSN en la siguiente sección.

Redes de Conmutación de Paquetes

Introducción a las PSN

En primer lugar, las PSN son redes de conmutación de paquetes de acceso público, también conocidas como PSDN, PSDCN, PSS y VAN, entre otros nombres. Consulta las siglas en la práctica tabla de referencia de siglas.

Las PSN X.25 más conocidas son: Sprintnet (anteriormente Telenet), BT Tymnet (la mayor) y Datapac (la más grande de Canadá). Todas estas redes tienen ventajas y desventajas, pero te diré esto: Si te encuentras en los Estados Unidos empieza con Sprintnet. Si estás en Canadá, Datapac es para ti.

Son muchas las razones por las que las PSN son tan populares entre los hackers. Literalmente existen miles de sistemas en redes PSN en todo el mundo, a los que puedes acceder gratuitamente si cuentas con los recursos necesarios. Debido al enorme tamaño de las redes PSN públicas, es muy raro ser detectado por rastreo. Su rastreo también es complicado, especialmente si se realiza un mínimo esfuerzo para evitarlo.

Cómo funciona la conmutación de paquetes

La siguiente explicación se aplica en general a todas las formas de conmutación de paquetes, pero se centra específicamente en las redes PSN que operan con la serie de protocolos X.25, como Datapac y SprintNet (a diferencia de Internet, que operan según protocolos TCP/IP, no obstante el principio común es el mismo). Las redes de conmutación de paquetes son algo complejas, pero intentaré simplificar la tecnología lo suficiente para que sea fácil de entender.

El usuario se conecta a un puerto local de acceso público de su PSN, mediante una conexión telefónica. Configura los parámetros de comunicación con el servidor de red y listo.

A partir de entonces, todos los datos remitidos a través de la red son agrupados primero en paquetes, generalmente de 128 o 256 bytes. Estos paquetes se ensamblan mediante el proceso de ensamblaje/desensamblaje de paquetes, tarea que lleva a cabo el puerto de acceso público, también conocido como PAD (Ensamblador/Desensamblador de Paquetes) o DCE (Equipo de Comunicación de Datos o Equipo de Terminación de Circuito de Datos).

Los paquetes se remiten a través de la red hasta su destino mediante los distintos protocolos X, generalmente X.25 con la ayuda de X.28, X.29 y X.3, dentro de su red nacional doméstica, o X.75/X.121 si se remiten internacionalmente. La serie de protocolos X son los estándares aceptados por la CCITT. El sistema host (DTE: Equipo Terminal de Datos, también conocido como PAD) al que se ha conectado, recibe el paquete y lo descompone mediante el ensamblaje/desensamblaje de paquetes, transformándolo en datos comprensibles para el sistema. A continuación, el DTE recompone sus datos en respuesta al paquete y los envía de vuelta a través de la red a su PAD, que los descompone en datos legibles para usted, el usuario. ¡Y esta es la versión simplificada!

Internet

Introducción

Contrario a la creencia popular, Internet es una red de conmutación de paquetes; simplemente no es una red de conmutación de paquetes que opere con el protocolo X.25. Internet opera con los protocolos TCP/IP (por lo general), por eso a veces se la descarta como una red de conmutación de paquetes. De hecho, la predecesora de Internet, ARPANET, fue el primer experimento a gran escala con tecnología de conmutación de paquetes. Lo que entonces se llamaba Telenet surgió posteriormente.

La confusión proviene del desconocimiento de los principios de la conmutación de paquetes, que es simplemente un tipo de red, explicado con detalle técnico anteriormente. Sin importar qué protocolos utilice la red; si se utiliza la metodología de conmutación de paquetes, obviamente es una red de conmutación de paquetes.

Bien, ahora habrás notado que Internet tiene una sección bastante pequeña, lo cual es cierto. Las razones son muchas. Esta es una guía de hacking, no un tutorial de Internet, así que no incluí IRC, Archie ni nada parecido. Y la razón principal es que pasé casi el doble de tiempo en redes X.25 que en Internet. Aun así, decidí incluir los aspectos esenciales de Internet. A partir de ellos, podrás seguir adelante.

La siguiente sección se basa principalmente en mi experiencia personal, pero el archivo de Internet de Gatsby me ayudó un poco, sobre todo en lo referente a las clases de direcciones IP.

Cómo obtener acceso

Obtener acceso puede ser entre fácil y muy difícil, dependiendo de dónde vivas y de lo bueno (¡o afortunado!) que seas como hacker. En primer lugar, si vas a hackear en Internet, debes estar en un sistema con acceso completo a Internet, no solo al correo electrónico. Esto descarta a servicios comerciales como Compuserve y Prodigy.

La mayoría de las universidades y algunos institutos de los EE.UU. Cuentan con acceso a Internet. Averigua qué puedes hacer para conseguir una cuenta, legal o ilegalmente.

Algunos BBS ofrecen acceso completo a Internet por un precio bastante razonable, y esa sería una buena opción.

Si te encuentras en una zona con redes voluntarias FreeNet, tendrás acceso completo a Internet... ¡gratis! Consulta con hackers locales o en foros de PD para averiguar dónde está el FreeNet más cercano.

Algunas empresas ofrecen acceso a Internet, pero pagando una tarifa comercial. Consulta con los usuarios locales de Internet para ver qué opciones hay disponibles en tu zona.

Por último, puedes intentar acceder mediante hackeo. Toda vez que hackees un sistema, verifica si cuenta con una conexión a Internet. Normalmente, podrás hacer esto efectuando una enlace de prueba por medio de Telnet (lo que que se explicará más adelante).

FTP

FTP son las siglas de Protocolo de Transferencia de Ficheros, y es el principal método para edscargar ficheros remotos a tu propio sistema (normalmente, al sistema a través del cual te conectas a Internet).

Solo proporcionaré una breve descripción general, ya que FTP es bastante sencillo de utilizar, cuenta con manuales de ayuda en línea y documentación completa sin conexión en su BBS local de HP.

Para empezar, FTP se puede inicializar escribiendo 'ftp' en cualquier sistema que lo tenga instalado. La mayoría cuentan con él, incluso si no tienen conexión a Internet. Esta es una lección frustrante que más de un novato ha aprendido: si accedes ilegalmente a un sistema que tiene FTP o Telnet en línea, no necesariamente tendrá acceso a Internet (y generalmente no lo tiene). Por ejemplo, ciertos sistemas SunOS cuentan con dos conjuntos de utilidades FTP y Telnet: los comandos estándares de FTP y Telnet provistos se pueden usar para conexiones de red de área local, pero no para Internet. Para usar estas facilidades en Internet se utilizan un conjunto de comandos específicos, itelnet, iftp, e ifinger.

Al ingresar a la utilidad FTP, normalmente se encontrará con el prompt 'ftp>', y al escribir 'help' debería aparecer un pequeño conjunto de archivos de ayuda. Los comandos disponibles junto con los archivos de ayuda, varían según el sistema.

El procedimiento depende del tipo de sistema operativo remoto que estés utilizando, ya que también varía. Generalmente, lo siguiente que debes hacer es abrir una conexión con el sistema del que deseas obtener el archivo. Escribe “**open**” seguido del nombre de host o la dirección IP del sistema al que deseas conectarte (explicado más adelante).

A continuación, normalmente verás una pantalla de inicio de sesión. Si tienes un nombre de usuario en ese sistema, introdúcelo. Si no, prueba con el usuario “**anonymous**”. “Anonymous” es en la práctica una cuenta de invitado que viene integrada en algunos sistemas operativos actuales. Los administradores de sistemas más cuidadosos pueden deshabilitarla, por razones obvias. Sin embargo, si no se encuentra deshabilitada, se te pedirá una contraseña. Escribe cualquier cosa, no importa. Escribe algunas "d" si quieres, realmente no importa (aunque, por regla general, no te sientes sobre el teclado... puede que no le guste... escribe algo aburrido).

Luego, simplemente usa el comando "**get**" para obtener el archivo que deseas. Por lo general, es buena idea no colocar los archivos en un directorio donde puedan ser detectados... el administrador del sistema sospechará que algo anda mal si encuentra algunos archivos que supuestamente copió en su propio directorio. Lo que nos lleva a la siguiente sección... asigna nombres inofensivos a tus archivos, especialmente si son algo como archivos /etc/passwd o problemas de Phrack.

Una nota sobre el FTP de /etc/passwds: rara vez funciona. Sí, obtendrás un archivo /etc/passwd, pero rara vez en Internet será el archivo correcto /etc/passwd real. Primero, compruebe el tamaño del archivo. Si es de 300 bytes o menos, probablemente sea un sustituto. Sin embargo, Telnet obtendrá el verdadero /etc/passwd en la mayoría de los casos.

Ahora cierre la utilidad FTP y revisa los ficheros descargados. Asegúrese de eliminarlos cuando termine.

Telnet

Si bien FTP no tiene un equivalente real en las redes X.25, se podría equiparar telnet a un PAD privado. Telnet le permite conectarse y operar en sistemas de Internet a través de Internet como si estuviera conectado localmente.

Telnet se inicializa escribiendo '**telnet**' en su terminal. El comando operativo es, de nuevo, '**open**'. Escriba 'open' seguido del nombre de dominio o la dirección IP. Una vez conectado, verá una solicitud de inicio de sesión de algún tipo (normalmente...). Introduce un nombre de usuario si tienes uno; de lo contrario, puedes intentar crear uno mediante un hackeo o comprobar si el sistema acepta al usuario invitado *anonymous*, como se explica en la sección FTP.

Si todo va bien, debería tener una conexión remota. Lo que sigue depende del sistema al que esté conectado, como en cualquier otra red.

Nombres de dominio y direcciones IP

Introducción

Ofrecer una breve explicación para quienes no estén familiarizados con estos términos.

Ya sea mediante FTP o Telnet, se necesita uno de ellos para conectarse a un sistema remoto. La dirección IP puede equipararse a una dirección de usuario de red (NUD) de las redes X.25.

El *nombre de dominio* es una regla mnemotécnica, utilizada principalmente por comodidad, ya que suele ser más fácil de recordar.

Si desea buscar sistemas en Internet, suele ser mucho más fácil hacerlo por dirección IP, puesto que no conocerá la regla mnemotécnica de la mayoría de los sistemas. Las direcciones IP son combinaciones de 4 dígitos separadas por puntos. Ejemplos de direcciones:

> 192.88.144.3 (EFF) y 18.72.2.1 (MIT).

Las direcciones se clasifican en tres clases:

- Clase A: del 0 al 127
- Clase B: del 128 al 191
- Clase C: del 192 al 223

Los primeros sistemas de Internet pertenecen a la Clase A, pero es más común encontrar sistemas de Clase B o C. Además, muchos sistemas se ubican específicamente en los prefijos 128 o 192, en lugar de 184, 201, etc.

El escaneo de un conjunto de direcciones IP se puede realizar de varias maneras. Una de ellas consiste en elegir un prefijo, añadir dos números aleatorios de uno o dos dígitos y escanear la última parte. Por ejemplo: tome 192.15.43 y escanee el último dígito del 0 al 255. Desafortunadamente, la última parte (o las dos últimas partes en el caso de la Clase C) son puertos, lo que significa que puede que no encuentre nada o que dé con la respuesta correcta. Experimente a su gusto; después de un tiempo, encontrará su ritmo.

También puede conectarse a sistemas específicos usando el nombre de dominio, si lo conoce o puede adivinarlo. Para adivinar un nombre de dominio, necesitará conocer el nombre de la empresa u organización y el tipo de organización.

Esto es posible porque los nombres de host deben conformar el Sistema de Nombres de Dominio (DNS), lo que facilita mucho la adivinación. Una vez que tenga ambos, normalmente podrá hacer algunas conjeturas fundamentadas sobre el nombre de dominio. Algunas son más fáciles que otras.

En primer lugar, deberá comprender el principio de los dominios de nivel superior.

El nivel superior se encuentra al final de un nombre de dominio; En el caso de eff.org, el nivel superior es 'org'. En el caso de mit.edu, el nivel superior es 'edu'.

Los niveles superiores se dividen en varias categorías:

- com - instituciones comerciales
- org - organizaciones sin fines de lucro
- edu - centros educativos
- net - redes
- gov - sistemas gubernamentales (no militares)
- mil - militares no clasificados

Además de los códigos de país. Los códigos de país son dos letras que se utilizan para llamadas internacionales; el de EE. UU. es 'US', el de Brasil es 'BR'.

Determina a qué nivel superior pertenece el sistema y luego haz algunas suposiciones. Ejemplos:

compuserve.com
xerox.com
mit.edu
eff.org

Para obtener más información, sugiero consultar algunas de las guías impresas de Internet disponibles actualmente, así como el archivo de Gatsby en Internet, impreso en Phrack 33.

Redes X.25

A partir de ahora, la sección PSN de este archivo se dedica a tratar las redes X.25.

Utilizo el acrónimo PSN indistintamente con redes X.25, así que no confunda PSN con otros tipos de redes PSN. De aquí en adelante, todo se denomina X.25.

Direcciones de Usuario de Red

El equivalente a un número telefónico en las PSN son las NUA (Direcciones de Usuario de Red). Gracias al DNIC (Código de Identificación de Red de Datos), no existen dos iguales, y necesita saberlas para conectarse a sistemas en redes PSN de todo el mundo.

El formato para introducir la NUA varía según la red PSN. Por ejemplo, en Datapac es necesario incluir ceros, pero en Sprintnet no son necesarios. Tymnet utiliza NUA de 6 dígitos en lugar de los 8 estándar.

El formato estándar del número NUA es este:

PDDDDXXXXXXXXSS,MMMMMMMMMM

Donde:

- P es una característica (dígito) pre-DNIC
- D es el DNIC
- X es la NUA
- S es el LCN(Número de Canal Lógico, subdireccionado)
- M es el Nemónico

Dependiendo de su PSN y del lugar al que llame, es posible que se omitan varios segmentos.

Como vemos, la característica P suele ser un 0, pero en Datapac es un 1. Normalmente ni siquiera se indica como parte del NUA, pero debe incluirse obligatoriamente si realiza llamadas a una PSN distinta a la suya. Si desea conectarse dentro de su propio PSN, no es necesario colocar la característica pre-DNIC.

Los 4 dígitos representados con la letra D representan el DNIC, también conocido como DCC (Código de Datos del País). El DNIC es un código de país de 4 dígitos, que garantiza que cada NUA sea único en el mundo. El DNIC solo se utiliza para conectar con NUA internacionales. Si está en Datapac (DNIC 3020), no es necesario incluir el DNIC de Datapac al realizar llamadas a NUA dentro de Datapac, pero si está en otro PSN, debe incluir el DNIC para las llamadas a Datapac.

La X simboliza al NUA propiamente dicho, que es obligatorio, junto con la S opcional (subdireccionamiento).

Puede simplificar aún más el NUA usando este formato:

PPPXXXXX

Donde P es el prefijo del NUA y las X son el sufijo. El prefijo corresponde a un código de área en la mayoría de los casos, ya que los NUA dentro de ese prefijo se encuentran en una parte específica

del país que cubre la red telefónica pública conmutada (PSN). En el caso de Sprintnet, el prefijo corresponde directamente al código de área (es decir, todos los NUA con el prefijo 914 en Sprintnet están en Nueva York, al igual que todos los números de teléfono con el código de área 914 se encuentran en Nueva York).

El subdireccionamiento, representado por la S en el diagrama, es algo complejo de explicar. El subdireccionamiento se utiliza cuando lo desea el propietario del DTE y sirve para conectarse a un sistema específico interno (dentro del mismo NUA). Si hay más de un sistema en la misma NUA, es posible que deba acceder a ellos mediante subdirecciones.

Por ejemplo:

```
          NUA                SISTEMA
        PPPXXXXXSS
        ==========       ==================
 Int.1  12300456               Unix
 Int.2  123004561              VMS
 Int.3  1230045699             HP3000
```

En este ejemplo, la NUA normal es 12300456 (suponiendo que no se utilicen el DNIC ni el dígito pre-DNIC). Esta NUA te lleva a un interno con sistema Unix. Pero cuando se usa el LCN (Número de Canal Lógico, subdirección) 1, te lleva a un interno con VMS. Y la subdirección 99 te lleva a un interno con HP3000. Los sistemas en la NUA 12300456 pertenecen a la misma persona o empresa, que deseaba tener una sola NUA, pero al usar subdirecciones les resulta posible dar acceso a varios sistemas con una sola NUA. Las subdirecciones también se usan ocasionalmente como medida de seguridad adicional. Si accedes a un sistema que muestra un mensaje de error como "ERROR DE PROCEDIMIENTO REMOTO" o "DIRECTIVA REMOTA", necesitarás una subdirección o un mnemónico.

Puedes optar por recorrer todas las subdirecciones posibles, del 1 al 99, o si solo estás escaneando, te sugiero estas: 1, 2, 50, 51, 91, 98, 99.

Los mnemónicos, M, son otro tema complicado de explicar. No están documentados por los PSN; los descubrí por mi cuenta. Los mnemónicos también se usan para seleccionar sistemas en una misma NUA como una especie de selector de puerto, pero se usan más comúnmente como una especie de contraseña externa, lo que impide incluso ver el sistema en cuestión.

Los mismos mensajes de error que en los LCN aparecen para los mnemónicos, pero, de nuevo, incluso si puedes acceder a un sistema con una NUA estándar, es posible que exista un sistema al que solo se pueda acceder mediante un mnemónico. Aquí tienes una lista de mnemónicos de uso común:

```
SYSTEM CONSOLE BOARD MODEM DIALUP X25 X28 X29 HOST SYSTEM
```

Cómo evitar los sistemas de cobro revertido

PADs Privados y NUI

En ocasiones, en las redes PSN, te encontrarás con sistemas que muestran el mensaje de error «LLAMADA A COBRO RECHAZADA». Esto indica un sistema de cobro revertido.

Cuando conectas a un sistema en una red PSN, la llamada se cobra automáticamente a cobro revertido. Sin embargo, muchos administradores de sistemas no quieren pagar los cargos de

conexión, y si todos sus usuarios tienen NUI o TABLEROS privados, es recomendable que configuren su sistema para que utilice el cobro inverso, lo que les ahorra dinero y, además, actúa como una barrera de seguridad adicional contra intrusos.

Pero, de nuevo, esto se puede evitar utilizando una BBS privada o un NUI.

Antes de entrar en detalles, recuerda que un PAD privado es diferente del PAD de tu puerto de acceso público. Un PAD privado es un PAD que asume automáticamente todos los cargos de conexión. Por lo tanto, los sistemas de tarifado inversa le permitirán eludir la tarifado inversa, ya que usted acepta los cargos.

Los NUI (Identificadores de Usuario de Red) funcionan de la misma manera. Puede pensar en un NUI como... digamos, una tarjeta telefónica. Se le facturan todos los cargos realizados a la tarjeta telefónica (independientemente de quién los haya realizado; el propietario recibe la factura). Un NUI funciona de la misma manera. Los NUI son utilizados por usuarios legítimos que aceptan los cargos de conexión.

Pero, como suele ocurrir con los hackers, estos NUI son robados y utilizados para llamar a todos los NUA del mundo, y recibe la factura el propietario legítimo. Pero a diferencia de las tarjetas de crédito, normalmente no tendrá problemas al usar un NUI.

Sin embargo, como puede imaginar, son bastante difíciles de conseguir PAD y NUI privados. Si alguien logra obtener uno, normalmente no estará dispuesto a compartirlo. Así que, todo depende de ti; probablemente tendrás que encontrar el tuyo propio.

Los PAD solo se encuentran escaneando en PSN y hackeando sistemas en PSN. Existen programas en sistemas Unix y Primos, por ejemplo, que funcionan como PAD privados. Y hay algunos PAD privados que se configuran exclusivamente para ser un PAD privado. Pero estos casi siempre están protegidos con contraseña, así que depende de ti acceder.

Los NUI son algo parecido. Los NUI varían de un PSN a otro; algunos te avisarán si un NUI es incorrecto, permitiéndote adivinar uno, pero otros no.

Y, por supuesto, aún tienes que adivinar la contraseña. He oído historias de personas que roban NUI, pero no estoy seguro de creerlo del todo, y la seguridad de esta práctica es cuestionable.

Grupos de Usuarios Cerrados

Una de las medidas de seguridad más efectivas que he visto es el CUG (Grupo de Usuarios Cerrados). El CUG es lo que genera el mensaje "LLAMADA BLOQUEADA" al escanear en las redes PSN. Un CUG solo acepta llamadas al DTE desde NUA DCE específicos. Esto significa que si tu NUA no está en la lista de NUA aceptables, ni siquiera podrás ver el sistema. Sin embargo, los CUG no son para todos. Si tienes un sistema con muchos usuarios que llaman desde diferentes puntos, los CUG no son útiles. Y menos mal. Nunca he oído hablar de nadie que haya encontrado una forma de sortear un CUG. Tengo algunas teorías, pero...

Sprintnet

Ahora hablaré un poco más sobre las principales redes PSN de EE. UU. y Canadá, empezando por la más popular en Estados Unidos: Sprintnet.

Para encontrar un puerto indio público para Sprintnet, es posible que puedas encontrarlo en tu guía telefónica (busca Sprintnet) o en el servicio de información telefónica. Si no, intenta comunicarte con el Servicio al Cliente de Sprintnet al 1-800-336-0437. Este servicio probablemente solo funcione entre las 8:30 y las 17:00 (hora del este), aunque podría variar ligeramente.

Además, para obtener un número de datos para consultas durante la llamada, intente 1-800-424-9494 con los parámetros de comunicación 7/E/1 (o 8/N/1, si no me equivoco). Escriba <CR> dos veces. O @D para 2400 bps y presione Enter para que Sprintnet pueda configurar sus parámetros de comunicación.

Aparecerá un breve mensaje y luego la solicitud TERMINAL=.

Ante la solicitud TERMINAL=, escriba VT100 para emular el terminal VT100. Si usa una computadora personal, creo que D1 funciona, o simplemente <CR> para terminal tonta.

Luego, escriba "c mail". En la solicitud de nombre de usuario, escriba "phones", y para la contraseña, escriba "phones" nuevamente. A partir de ahí, el sistema funciona mediante menús.

Ahora que tienes el número de puerto de marcación pública de Sprintnet, conéctate como si fueras un BBS. Cuando se conecte, escribe los dos <CR> para 300/1200 bps o @D para 2400 bps. A continuación, se mostrará su mensaje de bienvenida, algo parecido a esto:

> SPRINTNET(o en algunos casos TELENET)
> 123 11A

(donde 123 es su código de área junto con el prefijo de dirección de Sprintnet y 11A es el puerto que está usando)

> TERMINAL=

(tipea lo que pusiste previamente, ej:VT100,D1,<ENTER>)

Cuando Sprintnet muestre el prompt @, sabrá que está conectado a un PAD público de Sprintnet y que puede introducir los NUA.

Como mencioné antes, los prefijos NUA de Sprintnet corresponden directamente a los códigos de área. Para escanear Sprintnet, simplemente tome un código de área y añádale los dígitos restantes, generalmente en secuencia. Dado que Sprintnet ignora los ceros, los NUA pueden tener tan solo 4 dígitos. Al escanear, vaya del más bajo al más alto, deteniéndose en cuanto vea que se han agotado los NUA (intente con cien NUA más para asegurarse; lo mejor es llegar hasta 2000, o incluso más si tiene tiempo).

BT Tymnet

BT Tymnet pertenece a British Telecom y es, con diferencia, la mayor red conmutada de datos, pero cuenta con medidas de seguridad adicionales. Para encontrar los números de acceso telefónico de Tymnet, el procedimiento es muy similar: busque en la guía telefónica bajo Tymnet o BT Tymnet, o en el servicio de información telefónica y pregunte por los números de puerto de marcación pública de BT Tymnet. También puede llamar al servicio de atención al cliente de Tymnet al 1-800-336-0149. Generalmente, intente llamar entre las 8:30 y las 17:00 (hora del este). No tengo el número de datos de Tymnet para encontrar los números de acceso telefónico, pero una vez conectado a Tymnet, escriba INFORMATION para obtener una lista completa de los números de acceso

telefónico y otra información. Una vez que tenga su número de acceso telefónico, configure los parámetros de comunicación en 8/N/1 o 7/E/1 y disque el número como lo haría en un BBS. Al conectar, verá una cadena de caracteres extraños o nada. Pulse <CR> para que Tymnet sea capaz de autoconfigurar sus parámetros de comunicación. A continuación, verá el mensaje de ingreso a Tymnet, similar a este:

> -2373-001-
> please type your terminal identifier

Si le solicita un identificador de terminal, pulse A (si lo desea, puede pulsar A en lugar de <CR> al conectar para que el PAD de Tymnet pueda comparar sus parámetros de comunicación y obtener su identificador de terminal ASCII de una sola vez).

Tras esta parte inicial, verá el mensaje:

> please log in:

Esto indica que Tymnet está listo para que introduzca sus NUA. Sin embargo, muchos de los NUA en Tymnet se refieren en formato mnemotécnico. Para acceder a ellos, simplemente introduce el mnemotécnico que desees, sin nada más (por ejemplo: CPU o SYSTEM). Para introducir NUA digitales, necesita un NUI. Tymnet le avisará si el NUI que ingresa es incorrecto. Sigue probando con diferentes NUI y contraseñas hasta encontrar una correcta. Pero ten en cuenta que una de las principales medidas de seguridad de Tymnet es la siguiente: te desconectará luego de tres intentos fallidos. Por lo tanto, deberás volver a discar una y otra vez, y si utilizas un sistema de conmutación digital como ESS, no es recomendable llamar a ningún sitio durante demasiado tiempo. Así que úsalo con moderación si decides probar Tymnet.

Datapac

Me encanta Datapac, porque crecí usándolo. Casi todo el hackeo que he hecho hasta ahora ha sido en Datapac o en las PSN internacionales a las que he podido acceder mediante dispositivos privados que he encontrado en Datapac.

Para conectarte a la red Datapac desde Canadá, tendrás que discar a tu nodo Datapac local, al que puedes acceder en la mayoría de las ciudades a través de tu número de acceso telefónico local de Datapac.

Existen varias maneras de descubrir tu número de acceso telefónico local de Datapac. Normalmente lo encontrarás en tu guía telefónica bajo "PUERTO DE MARCACIÓN PÚBLICA DE DATAPAC". Si no, puedes buscarlo en la información telefónica con el mismo nombre. Como alternativa, existen un par de líneas telefónicas con módem para encontrar su puerto de marcación (estos también son para asistencia al cliente):

- 1-800-267-6574 (dentro de Canadá)
- 1-613-781-6798

Estos números solo funcionan de 8:30 a 17:00 EST (Hora Estándar del Este).

El Servicio de Información de Datapac (DIS) está en el NUA 92100086, y tiene un listado completo de todos los puertos de marcación públicos.

Puede usar ambas configuraciones de parámetros de comunicación, según creo, pero 8/N/1 (8 bits de datos, sin paridad, 1 bit de parada) es la más comúnmente utilizada, así que inicialmente configura dicho valores. Algunas NUA en Datapac usan 7/E/1; cámbiela si es necesario después de conectarse a un puerto de marcación de Datapac. Bien, si ya tienes tu número de teléfono público Datapac 3000 y has configurado los parámetros de comunicación en 8/N/1, ya puedes empezar.

Disca tu número como si fuera un BBS (obviamente) y, una vez conectado verás una pantalla en blanco. Escribe tres puntos ("..." y pulsa Intro (esto le indica a Datapac que se inicialice).

Aparecerá el mensaje de Datapac:

> DATAPAC: XXXX XXXX (el NUA de tu número).

Ya puedes introducir comandos en Datapac.

Ejemplo:

> atdt 16046627732 → tú lo introduces
>
> … → tú lo introduces
>
> DATAPAC: 6710 1071 → Respuesta de Datapac.

Ahora puedes introducir el NUA de tu destino.

Los NUA en Datapac deben tener entre 8 y 10 dígitos (sin incluir los mnemónicos). Por lo normal son 8, pero es posible tener que ingresar 9 o 10 dígitos, dependiendo del uso de subdirecciones.

Los prefijos NUA en Datapac se distribuyen en bloques, lo que significa que no corresponden a códigos de área, pero al observar los prefijos circundantes, se puede determinar la ubicación de un prefijo. Al escanear en Datapac, tenga en cuenta que la mayoría de los prefijos NUA válidos se encuentran en los números bajos, por lo que para muestrear un prefijo, vaya desde (por ejemplo) 12300001 hasta 12300200. Sin embargo, es recomendable escanear el prefijo hasta el 2000; la decisión es suya.

Listado de DNIC

He aquí un listado con los DNIC de PSN locales, y la mayoría de los demás DNIC de PSN de todo el mundo. Esta lista se descargó del DIS de Datapac, con algunas adiciones propias que se omitieron (el DIS no incluía otros PSN canadienses ni estadounidenses). Los DNIC adicionales provienen de mi propia experiencia y de listados obtenidos en varias BBS.

PAIS	RED	DNIC	DIRECCION
ANDORRA	ANDORPAC	2945	BI-DIR
ANTIGUA	AGANET	3443	INCOMING
ARABIA SAUDITA	ALWASEED	4201	BI-DIR
ARGENTINA	ARPAC	7220	BI-DIR
	ARPAC	7222	BI-DIR
AUSTRIA	DATEX-P	2322	BI-DIR
	DATEX-P TTX	2323	BI-DIR
	RA	2329	BI-DIR
AUSTRALIA	AUSTPAC	5052	BI-DIR
	OTC DATA ACCESS	5053	BI-DIR
AZORES	TELEPAC	2680	BI-DIR
BAHAMAS	BATELCO	3640	BI-DIR
BAHRAIN	BAHNET	4263	BI-DIR
BARBADOS	IDAS	3423	BI-DIR
BELGIUM	DCS	2062	BI-DIR
	DCS	2068	BI-DIR
	DCS	2069	BI-DIR
BELIZE	BTLDATAPAC	7020	BI-DIR
BERMUDA	BERMUDANET	3503	BI-DIR
BRASIL	INTERDATA	7240	BI-DIR
	RENPAC	7241	BI-DIR
	RENPAC	7248	INCOMING
	RENPAC	7249	INCOMING
BULGARIA	BULPAC	2841	BI-DIR
BURKINA FASO	BURKIPAC	6132	BI-DIR
CAMERÚN	CAMPAC	6242	BI-DIR
CANADA	DATAPAC	3020	BI-DIR
	GLOBEDAT	3025	BI-DIR
	CNCP PACKET NET	3028	BI-DIR
	CNCP INFO SWITCH	3029	BI-DIR
ISLAS CAIMÁN	IDAS	3463	BI-DIR
CHAD	CHADPAC	6222	BI-DIR
CHILE	ENTEL	7302	BI-DIR
	CHILE-PAC	7303	INCOMING
	VTRNET	7305	BI-DIR
	ENTEL	7300	INCOMING
CHINA	PTELCOM	4600	BI-DIR
COLOMBIA	COLDAPAQ	7322	BI-DIR
COSTA RICA	RACSAPAC	7120	BI-DIR
	RACSAPAC	7122	BI-DIR
	RACSAPAC	7128	BI-DIR
	RACSAPAC	7129	BI-DIR
CUBA	CUBA	2329	BI-DIR
CURACAO	DATANET-1	3621	BI-DIR
CHIPRE	CYTAPAC	2802	BI-DIR
	CYTAPAC	2807	BI-DIR
	CYTAPAC	2808	BI-DIR
	CYTAPAC	2809	BI-DIR
DINAMARCA	DATAPAK	2382	BI-DIR

	DATAPAK	2383	BI-DIR
DJIBOUTI	STIPAC	6382	BI-DIR
REP. DOMINICANA	UDTS-I	3701	INCOMING
EGIPTO	ARENTO	6020	BI-DIR
ESTONIA	ESTPAC	2506	BI-DIR
ESPAÑA	TIDA	2141	BI-DIR
	IBERPAC	2145	BI-DIR
FIJI	FIJIPAC	5420	BI-DIR
FINLANDIA	DATAPAK	2441	BI-DIR
	DATAPAK	2442	BI-DIR
	DIGIPAK	2443	BI-DIR
FRANCIA	TRANSPAC	2080	BI-DIR
	NTI	2081	BI-DIR
	TRANSPAC	2089	BI-DIR
	TRANSPAC	9330	INCOMING
	TRANSPAC	9331	INCOMING
	TRANSPAC	9332	INCOMING
	TRANSPAC	9333	INCOMING
	TRANSPAC	9334	INCOMING
	TRANSPAC	9335	INCOMING
	TRANSPAC	9336	INCOMING
	TRANSPAC	9337	INCOMING
	TRANSPAC	9338	INCOMING
	TRANSPAC	9339	INCOMING
ANTILLAS FR	TRANSPAC	2080	BI-DIR
GUAYANA FR	TRANSPAC	2080	BI-DIR
POLINESIA FR	TOMPAC	5470	BI-DIR
GABON	GABONPAC	6282	BI-DIR
ALEMANIA FED	DATEX-P	2624	BI-DIR
	DATEX-C	2627	BI-DIR
GRECIA	HELPAK	2022	BI-DIR
	HELLASPAC	2023	BI-DIR
GROENLANDIA	KANUPAX	2901	BI-DIR
GUAM	LSDS-RCA	5350	BI-DIR
	PACNET	5351	BI-DIR
GUATEMALA	GUATEL	7040	INCOMING
	GUATEL	7043	INCOMING
HONDURAS	HONDUTEL	7080	INCOMING
	HONDUTEL	7082	BI-DIR
	HONDUTEL	7089	BI-DIR
HONG KONG	INTELPAK	4542	BI-DIR
	DATAPAK	4545	BI-DIR
	INET HK	4546	BI-DIR
HUNGRIA	DATEX-P	2160	BI-DIR
	DATEX-P	2161	BI-DIR
ISLANDA	ICEPAK	2740	BI-DIR
INDIA	GPSS	4042	BI-DIR
	RABMN	4041	BI-DIR
	I-NET	4043	BI-DIR
INDONESIA	SKDP	5101	BI-DIR
IRLANDA	EIRPAC	2721	BI-DIR
	EIRPAC	2724	BI-DIR
ISRAEL	ISRANET	4251	BI-DIR
ITALIA	DARDO	2222	BI-DIR
	ITAPAC	2227	BI-DIR
COSTA DE MARFIL	SYTRANPAC	6122	BI-DIR
JAMAICA	JAMINTEL	3380	INCOMING
JAPÓN	GLOBALNET	4400	BI-DIR
	DDX	4401	BI-DIR
	NIS-NET	4406	BI-DIR
	VENUS-P	4408	BI-DIR
	VENUS-P	9955	INCOMIMG
	VENUS-C	4409	BI-DIR
	NI+CI	4410	BI-DIR

KENYA	KENPAC	6390	BI-DIR
COREA DEL SUR	HINET-P	4500	BI-DIR
	DACOM-NET	4501	BI-DIR
	DNS	4503	BI-DIR
KUWAIT	BAHNET	4263	BI-DIR
LÍBANO	SODETEL	4155	BI-DIR
LIECHTENSTEIN	TELEPAC	2284	BI-DIR
	TELEPAC	2289	BI-DIR
LUXEMBURGO	LUXPAC	2704	BI-DIR
	LUXPAC	2709	BI-DIR
MACAO	MACAUPAC	4550	BI-DIR
MADAGASCAR	INFOPAC	6460	BI-DIR
MADEIRA	TELEPAC	2680	BI-DIR
MALASIA	MAYPAC	5021	BI-DIR
MAURICIO	MAURIDATA	6170	BI-DIR
MEXICO	TELEPAC	3340	BI-DIR
MARRUECOS	MOROCCO	6040	BI-DIR
MOZAMBIQUE	COMPAC	6435	BI-DIR
PAÍSES BAJOS	DATANET-1	2040	BI-DIR
	DATANET-1	2041	BI-DIR
	DABAS	2044	BI-DIR
	DATANET-1	2049	BI-DIR
N. MARIANAS	PACNET	5351	BI-DIR
NUEVA CALEDONIA	TOMPAC	5460	BI-DIR
NUEVA ZELANDA	PACNET	5301	BI-DIR
NIGER	NIGERPAC	6142	BI-DIR
NORUEGA	DATAPAC TTX	2421	BI-DIR
	DATAPAK	2422	BI-DIR
	DATAPAC	2423	BI-DIR
PAKISTAN	PSDS	4100	BI-DIR
PANAMA	INTELPAQ	7141	BI-DIR
	INTELPAQ	7142	BI-DIR
PAPUA-NUEVA GUINEA	PANGPAC	5053	BI-DIR
PARAGUAY	ANTELPAC	7447	BI-DIR
PERU	DICOTEL	7160	BI-DIR
FILIPINAS	CAPWIRE	5150	INCOMING
	CAPWIRE	5151	BI-DIR
	PGC	5152	BI-DIR
	GLOBENET	5154	BI-DIR
	ETPI	5156	BI-DIR
POLONIA	POLAK	2601	BI-DIR
PORTUGAL	TELEPAC	2680	BI-DIR
	SABD	2682	BI-DIR
PUERTO RICO	UDTS	3300	BI-DIR
	UDTS	3301	BI-DIR
QATAR	DOHPAC	4271	BI-DIR
REUNION (FR)	TRANSPAC	2080	BI-DIR
RUANDA	RWANDA	6352	BI-DIR
SAN MARINO	X-NET	2922	BI-DIR
SENEGAL	SENPAC	6081	BI-DIR
SEYCHELLES	INFOLINK	6331	BI-DIR
SINGAPUR	TELEPAC	5252	BI-DIR
	TELEPAC	5258	BI-DIR
SOLOMON ISLANDS	DATANET	5400	BI-DIR
SOUTH AFRICA	SAPONET	6550	BI-DIR
	SAPONET	6551	BI-DIR
	SAPONET	6559	BI-DIR
SRI-LANKA	DATANET	4132	BI-DIR
SUECIA	DATAPAK TTX	2401	BI-DIR
	DATAPAK-2	2403	BI-DIR
	DATAPAK-2	2407	BI-DIR
SUIZA	TELEPAC	2284	BI-DIR
	TELEPAC	2285	BI-DIR
	TELEPAC	2289	BI-DIR

TAIWAN	PACNET	4872	BI-DIR
	PACNET	4873	BI-DIR
	UDAS	4877	BI-DIR
CHECOSLOVAQUIA	DATEX-P	2301	BI-DIR
TAILANDIA	THAIPAC	5200	BI-DIR
	IDAR	5201	BI-DIR
TONGA	DATAPAK	5390	BI-DIR
TOGOLESE REP.	TOGOPAC	6152	BI-DIR
TORTOLA	IDAS	3483	INCOMING
TRINIDAD	DATANETT	3745	BI-DIR
	TEXTET	3740	BI-DIR
TUNEZ	RED25	6050	BI-DIR
TURQUÍA	TURPAC	2862	BI-DIR
	TURPAC	2863	BI-DIR
TURKS&CAICOS	IDAS	3763	INCOMING
U ARAB EMIRATES	EMDAN	4241	BI-DIR
	EMDAN	4243	BI-DIR
	TEDAS	4310	INCOMING
URUGUAY	URUPAC	7482	BI-DIR
	URUPAC	7489	BI-DIR
USSR	IASNET	2502	BI-DIR
U.S.A.	WESTERN UNION	3101	BI-DIR
	MCI	3102	BI-DIR
	ITT/UDTS	3103	BI-DIR
	WUI	3104	BI-DIR
	BT-TYMNET	3106	BI-DIR
	SPRINTNET	3110	BI-DIR
	RCA	3113	BI-DIR
	WESTERN UNION	3114	BI-DIR
	DATAPAK	3119	BI-DIR
	PSTS	3124	BI-DIR
	UNINET	3125	BI-DIR
	ADP AUTONET	3126	BI-DIR
	COMPUSERVE	3132	BI-DIR
	AT&T ACCUNET	3134	BI-DIR
	FEDEX	3138	BI-DIR
	NET EXPRESS	3139	BI-DIR
	SNET	3140	BI-DIR
	BELL SOUTH	3142	BI-DIR
	BELL SOUTH	3143	BI-DIR
	NYNEX	3144	BI-DIR
	PACIFIC BELL	3145	BI-DIR
	SWEST BELL	3146	BI-DIR
	U.S. WEST	3147	BI-DIR
	CENTEL	3148	BI-DIR
	FEDEX	3150	BI-DIR
U.S. VIRGIN I	UDTS	3320	BI-DIR
U. KINGDOM	IPSS-BTI	2341	BI-DIR
	PSS-BT	2342	BI-DIR
	GNS-BT	2343	BI-DIR
	MERCURY	2350	BI-DIR
	MERCURY	2351	BI-DIR
	HULL	2352	BI-DIR
VANUATU	VIAPAC	5410	BI-DIR
VENEZUELA	VENEXPAQ	7342	BI-DIR
YUGOSLAVIA	YUGOPAC	2201	BI-DIR
ZIMBABWE	ZIMNET	6484	BI-DIR

Penetración de Sistemas

Bien, ahora que con suerte has encontrado algunos sistemas, necesitarás saber cómo identificarlos y, con un poco de suerte, acceder a ellos.

A continuación, encontrarás un listado de muchos sistemas operativos comunes como pude encontrar. Las nombres de usuario para cuentas enumeradas allí no son, propiamente dichas, "predeterminadas". Hay muy pocas cuentas predeterminadas reales. Son "cuentas comunes" porque es probable que muchas de ellas estén presentes. Así que, pruébalas todas, puede que tengas suerte.

La lista de cuentas comunes nunca estará completa, pero la mía es bastante aproximada. He hackeado una cantidad increíble de sistemas y, gracias a ello, he podido recopilar una lista bastante extensa de cuentas comunes.

En los casos donde dejé el espacio de contraseña en blanco, simplemente prueba con el nombre de usuario (y cualquier otra cosa que quieras), ya que no hay contraseñas comunes aparte del nombre de usuario.

Además, en el espacio de contraseña nunca incluí el nombre de usuario como contraseña, ya que es seguro que lo intentarás.

Recuerda que las contraseñas que se proporcionan son solo sugerencias; prueba con la que quieras.

UNIX

Unix es uno de los sistemas operativos más extendidos del mundo. Si revisas una PSN, es probable que encuentres varias instalaciones de Unix, sin importar en qué parte del mundo se encuentre la PSN.

El mensaje de inicio de sesión predeterminado para un sistema Unix es 'login', y aunque no se puede cambiar, se pueden agregar caracteres adicionales al principio de 'login', como 'rsflogin:'. Presiona <CR> varias veces y debería desaparecer.

Como UNIX es un software no propietario, existen muchas variantes, como Xenix, SCO, SunOS, BSD, etc., pero el sistema operativo se mantiene prácticamente igual.

Por regla general, los nombres de usuario y las contraseñas de UNIX se ecriben solo en minúsculas, aunque Unix distingue entre mayúsculas y minúsculas, así que puedes experimentar si no tienes suerte. Generalmente, se permiten 4 intentos para iniciar sesión con una contraseña, pero este número puede aumentarse o disminuirse a discreción del administrador del sistema.

Desafortunadamente, UNIX no avisa cuando el nombre de usuario que has introducido es incorrecto. UNIX sólo informa al usuario de cuándo se realizó el último intento de inicio de sesión fallido, pero nada más. Sin embargo, el administrador del sistema puede mantener registros y pistas de auditoría si así lo desea, así que ten cuidado.

Dentro de un sistema UNIX, escribe 'cat /etc/passwd'. Esto te dará la lista de nombres de usuario y las contraseñas cifradas.

El comando 'who' muestra una lista de usuarios conectados. 'Learn' y 'man' abren la ayuda.

Una vez dentro, normalmente verás el prompt $ o % para usuarios normales, o # para superusuarios.

La cuenta root es el superusuario, por lo que la contraseña puede ser cualquiera y probablemente esté bien protegida. Dejé este espacio en blanco; tú decides. No habrá contraseñas comunes para root.

Cuentas comunes

Nombre de Usuario	Contraseña
root	
daemon	
adm	admin, sysadm, sysadmin, operator, manager
uucp	
bin	
sys	
123	lotus, lotus123
adduser	
admin	adm,sysadm,sysadmin,operator,manager
anon	anonymous
anonuucp	anon, uucp, nuucp
anonymous	anon
asg	device devadmin
audit	
auth	
backappl	
backup	save, tar
batch	
bbx	
blast	
bupsched	
cbm	
cbmtest	
checkfsys	
control	
cron	
csr	support, custsup
dbcat	database, catalog
default	user, guest
demo	tour, guest
dev	
devel	
devshp	
diag	sysdiag, sysdiags, diags, test
diags	diag, sysdiag, sysdiags
dialup	
dos	
fax	
field	fld, service, support, test
filepro	
finger	
fms	
friend	guest, visitor
games	
general	
gp	
gsa	
guest	visitor, demo, friend, tour
help	
host	
hpdb	
info	
informix	database
ingres	database

```
inquiry
install
journal
journals
kcml
learn
lib                library, syslib
link
listen
lp                 print spooler lpadmin
lpadmin            lp, adm, admin
lpd
ls
mail
maint              sysmaint, service
makefsys
man
manager            mgr, man, sysmgr, sysman, operator
mdf
menu
mountfsys
ncrm               ncr
net                network
netinst            inst, install, net, network
netman             net, man, manager, mgr, netmgr, network
netmgr             net, man, manager, mgr, netmgr, network
network            net
newconv
news
nobody             anon
nuucp              anon
oasys              oa
odt                opendesktop
online
openmail           mail
oper               operator,manager,adm,admin,sysadmin,mgr
operator           sysop, oper, manager
opp
oracle             database
oraclev5           oracle, database
oradev             oracle
pcs
pcsloc
pctest
postmaster         mail
powerdown          shutdown
priv               private
prod
pub                public
public             pub
reboot
remote
report
rha
rje
rsm
rsmadm             rsm, adm, admin
rusr
sales
sas
save               backup
savep
service            field, support
setup
```

```
shutdown
smtp              mail
softwork
space
startup
su
sundiag           sysdiag, diag, diags, sysdiags
suoper            su, oper, operator
super             supervisor, manager, operator
support           field, service
sync
sysadm            adm, admin, operator, manager
sysdiag           diag, diags, sysdiags
sysinfo           info
sysmaint          maint, service
sysman            manager,mgr,man,admin,operator,sysadmin
sysmgr            manager,mgr,man,admin,operator,sysadmin
system            sys, unix, shell, syslib, lib, operator
systest           test, tester, testuser, user
test              tester, testuser, systest, user
tester            test, user, testuser
testuser          test, tester, user, systest
tftp
tour              demo, guest, user, visitor
transfer
tty
tutor
tutorial
umountfsys
unix
unixmail          mail, unix
user              guest, demo
userp             user
usr               user
usrlimit
utest
uucpadm           adm, admin, uucp
uuadm             uucp, adm
uuadmin           uucp, admin
uuhost            uucp, host
uulog             uucp, log
uunx              uucp
uupick            uucp, pick
uustat            uucp, stat
uuto              uucp, to
uux               uucp
va
vashell
vax
visitor           guest, friend, demo, tour
vlsi
vmsys             vm, face
vsifax
who
wp
wp51
x25               pad
x25test           test
x400
```

VMS

El Sistema de Memoria Virtual VMS corre comúnmente en computadoras DEC VAX. Es otro sistema muy extendido, con muchos usuarios en todo el mundo.

VMS mostrará un mensaje solicitando ingresar el nombre de usuario. Para asegurarse, simplemente introduce una coma (,) como nombre de usuario. VMS mostrará un mensaje de error si se cumplen ciertos límites. Normalmente, tendrá tres intentos de inicio de sesión, y VMS no le avisará si ha ingresado un nombre de usuario incorrecto.

Una vez dentro, verá el símbolo $.

Cuentas Comunes

Username	Password
backup	
batch	
dcl	
dec	
decmail	mail
decnet	
default	default, user
dialup	
demo	guest
dsmmanager	dsm, manager
dsmuser	dsm, user
field	field, service, support, test, digital
games	
guest	visitor, demo
help	
helpdesk	
help_desk	helpdesk
host	
info	
ingres	database
interactive	
link	
local	
mail	
mailer	mail
mbmanager	mb, manager, mgr, man
mbwatch	watch, mb
mpdbadmin	mpdb, admin
netcon	net, network
netmgr	net, manager, mgr, operator
netpriv	network, private, priv, net
netserver	
network	net
newingres	ingres
news	
operations	operations
operator	oper, manager, mgr, admin,
opervax	operator, vax
ops	
oracle	
pcsdba	
pfmuser	pfm, user
postmaster	mail
priv	private
remote	
report	

```
rje                 remote, job, entry
student
suggest             suggest
sys
sysmaint            sysmaint, maint, service, digital
system              manager,operator,sys,syslib
systest             uetp,test
systest_clig        systest, test
tapelib
teledemo            demo
test                testuser, tester
uetp
user                test, guest, demo
userp               user
vax
vms
visitor             guest, demo
wpusers
```

HP3000

Los mainframes HP3000 corren la serie de sistemas operativos MPE, tales como MPE, V, ix, X y XL.

El mensaje de inicio de sesión predeterminado es ':', pero puede ir precedido de caracteres (por ejemplo: 'mentor:') y, en algunos casos, los ':' pueden eliminarse por completo (por ejemplo: 'mentor'). Para comprobar si se trata de un HP3000, pulsa <CR>. Aparecerá un mensaje de error como este:

> EXPECTED HELLO, :JOB, :DATA, OR (CMD) AS LOGON. (CIERR 1402)

Para iniciar sesión, escriba '**hello**', seguido de la información de inicio de sesión, que tiene este formato: USUARIO.CUENTA,GRUPO. El grupo es opcional, pero puede ser necesario en algunos casos y puede proporcionar diferentes conjuntos de archivos y su ordenación.

Una gran ventaja de los HP3000 es que te indican exactamente qué es incorrecto en el nombre de usuario que les has proporcionado, ya sea que la cuenta sea válida pero el nombre de usuario sea incorrecto, o al revés. Pero, lamentablemente, si los operadores del sistema lo desean, pueden proteger con contraseña TODOS los segmentos del nombre de usuario: nombre de usuario, cuenta y grupo.

El prompt interno de comandos para MPE es, de nuevo, :.

La opción "Help" te brindará asistencia dentro de un HP3000.

Al ingresar cuentas, al principio sugiero no usar un grupo. Si recibes el mensaje de error "no está en el grupo principal", intenta con el grupo PUB; si incluso eso falla, pasa a la lista de grupos comunes.

No incluí las contraseñas junto con las cuentas, ya que el formato sería un poco incómodo debido al formato poco convencional de MPE. Las únicas contraseñas predeterminadas del fabricante que conozco son 'hponly' para mgr.telesup, 'lotus' para mgr.sys y 'hpword' para field.support.

Recuerda probar las distintas partes de la cuenta como contraseña, y cualquier otra similar.

Si necesitas una contraseña para las siguientes cuentas de usuario y grupos, prueba las distintas partes del nombre, además de combinaciones del mismo o nombres con vínculos obvios (por ejemplo: field=service).

Cuentas Comunes:

```
NombreUsuario.Cuenta
--------------------
mgr.3000devs
mgr.acct
mgr.backup
manager.blast
manager.blast1
mgr.ccc
spool.ccc
mgr.cnas
manager.cognos
mgr.cognos
operator.cognos
mgr.common
mgr.company
mgr.conv
mgr.corp
mgr.cslxl
mgr.demo
operator.disc
mgr.easy
mgr.easydev
mgr.extend
mgr.hpdesk
mgr.hplanmgr
field.hpncs
mgr.hpncs
advmail.hpoffice
deskmon.hpoffice
mail.hpoffice
mailman.hpoffice
mailroom.hpoffice
mailtrck.hpoffice
manager.hpoffice
mgr.hpoffice
openmail.hpoffice
pcuser.hpoffice
spoolman.hpoffice
x400fer.hpoffice
x400xfer.hpoffice
wp.hpoffice
mgr.hponly
mgr.hpoptmgt
field.hpp187
mgr.hpp187
mgr.hpp189
mgr.hpp196
mgr.hppl85
mgr.hppl87
mgr.hppl89
mgr.hppl96
mgr.hpskts
mgr.hpspool
mgr.hpword
mgr.hpx11
dpcont.hq
mgr.hq
```

```
mgr.indhpe
mgr.infosys
mgr.intx3
manager.itf3000
mail.mail
mgr.netbase
mgr.netware
operator.netware
mgr.orbit
mgr.prod
mgr.rego
mgr.remacct
mgr.rje
manager.security
mgr.security
mgr.sldemo
mgr.snads
mgr.softrep
mgr.speedwre
mgr.spool
manager.starbase
field.support
mgr.support
operator.support
exploit.sys
manager.sys
mgr.sys
operator.sys
pcuser.sys
rsbcmon.sys
operator.syslib
sysrpt.syslib
mgr.sysmgr
operator.system
mgr.tech
mgr.techxl
mgr.telamon
field.hpword
mgr.opt
manager.tch
field.telesup
mgr.telesup
sys.telesup
mgr.tellx
monitor.tellx
mgr.utility
mgr.vecsl
manager.vesoft
mgr.vesoft
mgr.word
field.xlserver
mgr.xlserver
mgr.xpress
```

Grupos Comunes:

```
admin
advmail
ask
brwexec
brwonlne
brwspec
```

bspadmin
bspdata
bspinstx
bsptools
catbin1
catbin2
catlib
classes
config
console
convert
creator
curator
currarc
current
dat
data
database
delivery
deskmon
devices
diadb
diag
diafile
diaipc
doc
docxl
document
dsg
easy
ems
emskit
etdaemon
example
examples
ezchart
galpics
graphics
hold
hpaccss
hpadvlk
hpadvml
hpdesk
hpdraw
hpecm
hpemm
hpenv
hpgal
hphpbkp
hplibry
hplist
hplt123
hpmail
hpmap
hpmenu
hpprofs
hpsw
hptelex
ibmpam
idl
idlc
idpxl
include
infoxl

instx
internal
itpxl
job
lib
libipc
library
mailconf
maildb
mailhelp
mailjob
maillib
mailserv
mailstat
mailtell
mailxeq
mediamgr
memo
memory
mgr
mmgrdata
mmgrxfer
mmordata
mmorxfer
monitor
mpexl
ndfiles
ndports
net
network
nwoconf
office
oldmail
oper
operator
out
pascalc
patchxl
pcbkp
ppcdict
ppcsave
ppcutil
prntmate
prog
prvxl
pub
pubxl
qedit
ref
request
restore
sample
sbase
sfiles
signal
sleeper
snax25
sql
sruntime
subfile
suprvisr
sx
sys
sysmgr

```
sysvol
tdpdata
telex
telexjob
text
tfm
ti
tools
transmit
user
users
validate
viewlib
visicalc
wp
wp3
x400data
x400db
x400fer
x400file
xspool
```

VM/CMS

El sistema operativo VM/CMS se encuentra instalado en mainframes de IBM, y aunque existen bastantes, suelen ser ignorados por hackers que prefieren Unix o VMS. Los sistemas VM/CMS suelen encontrarse protegidos mediante VTAM Sim3278 y sistemas ISM. El mensaje de inicio de sesión para CMS es '.', pero puede que se muestre información adicional antes del mensaje, como:

> Virtual Machine/System Product
> !
> .

o bien:

> VM/370
> !
> .

...y frecuentemente al costado:

```
LOGON userid
DIAL userid
MSG userid message
LOGOFF
```

...aunque todos representan un sistema VM/CMS.

Para iniciar sesión, escriba 'logon' seguido del nombre de usuario, que suele tener entre 1 y 8 caracteres. Para asegurarse de que es un CMS, escriba 'logon' seguido de cualquier texto aleatorio. Si es un VM/CMS, responderá:

> Userid not in CP directory

Esta es una de las grandes ventajas de los CMS: le indica si el ID de inicio de sesión que ingresó es incorrecto, lo que facilita la búsqueda de IDs válidos.

Tenga cuidado: si intenta realizar un ataque de fuerza bruta, algunos sistemas simplemente bloquearán la cuenta o incluso la función de inicio de sesión durante un tiempo. En ese caso, averigüe el límite y manténgase justo por debajo de él. Desconecte el operador o borre el circuito si es necesario, pero si bloquea continuamente las funciones de inicio de sesión, levantará sospechas antes de siquiera poder acceder.

Una vez dentro, al escribir 'help' encontrará un manual en línea de nivel intermedio.

Cuentas Comunes

Username	Password
$aloc$	
admin	operator, manager, adm, sysadmin, sysadm
alertvm	alert
ap2svp	
apl2pp	
autolog1	autolog
autolog2	autolog
batch	
batch1	batch
batch2	batch
botinstl	
ccc	
cms	
cmsbatch	cms, batch, batch1
cmsuser	cms, user
cpms	
cpnuc	
cprm	
cspuser	user, csp
cview	
datamove	
demo1	demo
demo2	demo
direct	
dirmaint	dirmaint1
diskcnt	
entty	
erep	
formplus	
fsfadmin	fsf, adm, sysadmin, sysadm, admin, fsfadm
fsftask1	
fsftask2	
gcs	
gcsrecon	
idms	
idmsse	
iips	
infm-mgr	infm, man, manager, mgr
inoutmgr	mgr, manager
ipfappl	
ipfserv	
ispvm	
ivpm1	
ivpm2	
maildel	
mailman	
maint	service
moeserv	
netview	network, view, net, monitor
oltsep	

```
op1
opbackup          backup
operatns          op, operator, manager, admin
operator          op, operatns, manager, admin
opserver
pdm470
pdmremi
peng
presdbm           dbm
procal
prodbm            prod
promail
psfmaint          maint
pssnews           news
pvm
router
rscs
rscsv2
savsys
sfcm1             sfcm
sfcntrl
sim3278
smart
sna
sqldba            database
sqluser           user, sql
syncrony
sysadmin          admin, adm, sysadm, manager, operator
sysckp
sysdump1          sysdump
syserr
syswrm
tdisk             disk, temp
temp
tsafvm
vastest           test
vm3812
vmarch
vmasmon
vmassys
vmbackup          backup
vmbsysad
vmmap             map
vmtape            tape
vmtest            test, testuser
vmtlibr
vmutil            util, utils
vseipo
vsemaint          maint
vseman
vsm
vtam
vtamuser          user, vtam
x400x25
```

PRIMOS

El sistema operativo Primos, que corre en los mainframes de la compañía Prime, es de uso bastante extendido y se encuentra comúnmente en redes de conmutación de paquetes en todo el mundo.

Al conectarse, recibirá una cabecera similar a:

PRIMENET 23.3.0 INTENG

Esto le informa que se trata de un ordenador Primos, el número de versión y el identificador del sistema que el propietario eligió, que suele ser el nombre de la empresa o la ciudad donde se encuentra el Primos.

Si encuentra un Primos en una red, recibirá la cabecera Primenet, pero si está fuera de una red, la cabecera puede ser diferente (por ejemplo: Primecon). Presione varias veces <CR> y Primos le mostrará el mensaje de inicio de sesión:

'ER!'.

En este punto, escriba 'login' seguido de su nombre de usuario. Si al presionar <CR> no aparece 'ER!', escriba 'login' seguido de su nombre de usuario.

Si tienes suerte y encuentras alguna empresa de la prehistoria que ejecute la versión 18.0.0 o inferior, tienes acceso garantizado. Solo necesitas un nombre de usuario y no te pedirá contraseña. Si por alguna razón se requiere contraseña, con un par de Control+C deberías poder acceder.

Desafortunadamente, Primos casi siempre permite un solo intento de combinación de nombre de usuario/contraseña antes de desconectarte, y no te avisará si la ID que has introducido es inválida.

Una vez dentro, verás el mensaje:

OK

"HELP" abre una guía de ayuda en línea regular.

Cuentas Comunes

Usuario	Password
backup	
backup_terminal	
batch_service	
batch	
bootrun	
cmdnc0	
demo	
diag	
dos	
dsmsr	dsm
dsm_logger	dsm
fam	
games	
guest	
guest1	guest
lib	
libraries	
login_server	
mail	
mailer	
netlink	net, primenet
netman	manager, man, mgr, netmgr
network_mgt	netmgt
network_server	server
prime	primos, system
primenet	net, netlink
primos	prime, system

```
primos_cs           primos, prime, system
regist
rje
spool
spoolbin            spool
syscol
sysovl
system              prime, primos, sys1, operator
system_debug
system_manager
tcpip_manager
tele
test
timer_progress
tools
```

TOPS-10/20:

Un sistema operativo antiguo y algo atípico, TOPS-10 corría en las máquinas DEC-10/20. Normalmente se puede reconocer un TOPS-10 por su prompt de comandos, un solo punto (.), mientras que un TOPS-20 tendrá un '@' en su lugar. La mayoría de los sistemas permiten introducir los comandos 'SYSTAT' o 'FINGER' desde el prompt de inicio de sesión, antes de iniciar sesión.

Este comando permite ver los usuarios en línea, una valiosa ayuda para el hacking.

Para iniciar sesión, escriba 'login xxx,yyy', donde x e y son dígitos. TOPS-10 le avisa cuando su nombre de usuario es incorrecto.

Cuentas Comunes

ID Code Usuario	Contraseña
1,2	OPERATOR, MANAGER, ADMIN, SYSLIB, LIB
2,7	MAINT, MAINTAIN, SYSMAINT
5,30	GAMES

IRIS

Lamentablemente, no tengo ninguna experiencia con IRIS. Hasta el día de hoy, ni siquiera he visto uno. Por lo tanto, con pesar debo presentar material antiguo. La siguiente información proviene íntegramente del Diario Técnico LOD/H n.° 3. Con suerte, seguirá siendo aplicable.

El sistema operativo IRIS solía ejecutarse exclusivamente en sistemas PDP, pero ahora se ejecuta en una gran variedad de máquinas.

IRIS suele presentarse con un mensaje como:

> "Welcome to IRIS R9.1.4 timesharing"

Y luego una solicitud de "ACCOUNT ID?".

IRIS le avisa cuando introduce un ID incorrecto, no lo desconecta después de demasiados intentos y no guarda registros. Y, curiosamente, ¡no se utilizan contraseñas! Así que, si puede conseguir un sistema operativo IRIS, pruebe la siguiente configuración predeterminada y debería funcionar.

Cuentas Comunes

```
Nombre de Usuario
-----------------
accounting
boss
demo
manager
noname
pdp8
pdp11
software
tcl
```

NOS

El NOS (Sistema Operativo de Red) se encuentra en los mainframes Cyber fabricados por la CDC (Control Data Corporation). Las máquinas Cyber suelen ser utilizadas por instituciones como universidades e instalaciones de investigación atómica. Los Cyber generalmente muestran algún tipo de identificador, como

> Sheridan Park Cyber 180-830 Computer System

o

> Sacramento Cyber 180-830 CSUS NOS Software System

La primera solicitud de inicio de sesión será 'FAMILY:', solo presione <CR>.

La siguiente solicitud es 'USER NAME:'. Esto es más difícil, generalmente consiste en una cadena de 7 caracteres. La contraseña es aún peor, generalmente 7 letras aleatorias. ¿Suena mal? Lo es. Intentar forzar una cuenta es prácticamente imposible.

Nunca he visto que estas contraseñas predeterminadas funcionen, pero son mejor que nada. Las obtuve de la Guía para principiantes de LOD/H sobre Hacking, escrita por el Mentor. No se conocen contraseñas para estos nombres de usuario.

Cuentas Comunes

```
Usuario
--------
$SYSTEM
SYSTEMV
```

DECSERVER

El Decserver, como su nombre indica, es un servidor fabricado por Digital Equipment Corporation, la misma empresa que fabrica las máquinas VAX.

Es posible que el propietario del servidor le haya puesto una contraseña; en ese caso, aparecerá el prompt de comandos #. Si el servidor tiene PADs o llamadas salientes, es muy probable que así sea.

No necesitas un nombre de usuario, solo la contraseña. Normalmente tendrás 3 intentos, pero se puede modificar. La contraseña predeterminada es 'access', pero otras buenas opciones para probar son: server, dec, network, net, system (y cualquier otra combinación).

Si superas el prompt de comandos #, o si no aparece ninguno, aparecerá el indicador 'Enter Username>'. Lo que escribas no importa, tan solo es un identificador. Escribe algo que suene normal, y no tu alias de hacker. Resulta interesante observar a los usuarios conectados a un Decserver, ya que es común encontrar algunos usuarios con nombres de usuario como C, CCC o similares, lo que suele indicar que probablemente sean otros hackers.

Además, en la solicitud Enter Username>, puede pedir ayuda con el comando "help", que genera un archivo de ayuda de inicio de sesión bastante extenso. Si todo va bien, debería aparecer la solicitud "Local>".

Los Decservers cuentan con un buen conjunto de archivos de ayuda; simplemente escriba "help" y lea todo lo que desee. Es recomendable ejecutar "show users" al iniciar sesión por primera vez, y luego "show services" y "show nodes". Los servicios son los ordenadores conectados al Decserver, a los que puede acceder. Por razones obvias, a menudo encontrará muchos sistemas VAX/VMS en los Decservers, pero prácticamente puede encontrar cualquier cosa.

Busque servicios con nombres como Dial, Modem, PAD, X25, Network o similares. Pruebe prácticamente todo que vea. Recuerde probar los nombres de usuario que aparecen al ejecutar "show users" como usuarios de los sistemas en línea.

Además, a veces encontrará que su Decserver tiene acceso a Internet (Telnet, SLIP o FTP); asegúrese de aprovecharlo al máximo.

Para conectarse a los servicios que ve, use 'c XXXX', siendo las X el nombre del servicio consultado. Una vez dentro, el valor predeterminado del fabricante para los privilegios es 'system' y rara vez se cambia.

La contraseña de mantenimiento cambia según la versión. En los Decserver 200 y 500 es 0000000000000000 (16 ceros), pero en el 300 es simplemente 0.

GS/1

El GS/1 es otro tipo de sistema de servidor, pero son menos comunes que los Decservers. El prompt predeterminado es 'GS/1>', pero se puede cambiar según las preferencias del administrador del sistema.

Para comprobar si hay un GS/1, ejecute 'sh d', que mostrará algunas estadísticas. Para ver qué sistemas están disponibles en el servidor, escriba 'sh n' o 'sh c', y 'sh m' para las macros del sistema.

XMUX

El XMUX es un sistema de multiplexación que proporciona acceso remoto, fabricado por Gandalf Technologies, Inc., Gandalf of Canada Ltd., en Canadá. Por lo que sé, el XMUX se utiliza únicamente en redes de conmutación de paquetes (Datapac en particular), pero también se usa en redes de conmutación de paquetes en todo el mundo. El XMUX no suele considerarse un sistema operativo independiente, sino más bien un sistema de soporte para sistemas de red multiusuario, relacionado con la monitorización del sistema, el control de canales y algunas de las funciones de multiplexación.

Por lo tanto, es común encontrar un XMUX en un mnemónico o una subdirección de otro sistema, aunque también se encuentran con frecuencia solos en su propia NUA.

Para encontrar los sistemas en una subdirección o un mnemónico, lo mejor es utilizar los mnemónicos, ya que el mnemónico LOGGER no se puede eliminar, mientras que el subdireccionamiento es opcional. No siempre querrás revisar todos los sistemas, así que te daré una guía sobre dónde buscar; (RECUERDA: esto solo aplica a los sistemas de PSN y puede que no se aplique a tu PSN).

- PACx/: El PACx/Starmaster también es fabricado por Starmaster Gandalf, y ambos sistemas están estrechamente interrelacionados. Si las mnemónicas no funcionan, asegúrese de probar las LCN, ya que la CONSOLE en un PACX/Starmaster es completamente diferente, y usar la mnemónica CONSOLE con frecuencia lo llevará a la consola PACX, no a la consola XMUX.
- Sistemas BBS: Los sistemas BBS en PSN a menudo necesitan ayuda, y los XMUX se encuentran con bastante frecuencia en ellos.
- Otros sistemas: Muchos otros sistemas operativos, como Unix, AOS/VS, Pick y HP3000, tienen XMUX ocasionalmente.
- En red: Una buena parte de los sistemas en red tienen XMUX de sistema.

Si un sistema también tiene un XMUX, puede acceder a él casi siempre mediante el mnemónico CONSOLE, y si no, mediante el nombre del nodo del XMUX. Si eso no funciona, pruebe con LCN hasta el 15 inclusive.

En ocasiones, la consola del XMUX no tendrá contraseña, en cuyo caso accederá directamente a ella. La consola del XMUX es intuitiva y tiene menús, así que le dejo que la explore.

Sin embargo, lo más probable es que se encuentre con la solicitud de contraseña, 'PASSWORD>'. Esta no se puede modificar, pero puede aparecer un aviso de una línea encima.

Para comprobar si hay un XMUX, simplemente pulse <CR>. Le indicará que la contraseña ha sido inválida y que debe contener entre 1 y 8 caracteres alfanuméricos.

Como puede ver, no necesita un nombre de usuario para la consola remota de un XMUX. Se utilizan UID, pero internamente dentro de la estación de trabajo.

Como se ha dicho, su formato de la contraseña es de 1 a 8 caracteres alfanuméricos. No hay contraseña predeterminada; la consola se deja sin protección a menos que el propietario decida protegerla con una contraseña.

Sin embargo, existen contraseñas comunes: console, gandalf, xmux, system, password, sys, mux, xmux1. Las repetiré más adelante en la sección de contraseñas comunes. Pero estas no siempre funcionarán, ya que depende del propietario elegir la contraseña (aunque suelen preferirlas). La siguiente mejor opción es averiguar el nombre del nodo del XMUX.

Los XMUX también son sistemas de sondeo, generalmente conectados de alguna manera a uno de los hubs regionales.

Para ello, debe comprender las partes del XMUX. El XMUX tiene 4 partes predeterminadas: CONSOLE, FOX, LOGGER y MACHINE. Intentaré definir un poco mejor su uso:

- CONSOLE: la parte remota principal del XMUX, que realiza todas las funciones de mantenimiento y del sistema propiamente dicho. Se suele acceder a través de la LCN (subdirección) 0 o 4/5, y el mnemónico predeterminado CONSOLE, que puede cambiarse.
- FOX: un sistema de prueba que ejecuta líneas interminables del alfabeto y los dígitos del 0 al 9. Se accede a través de la LCN 1, mnemónico FOX.
- LOGGER: un dispositivo que muestra información de registro, normalmente una o dos líneas, incluyendo el nombre del nodo. Se accede a través de la LCN 2, mnemónico LOGGER.
- MACHINE: un sistema que aún no comprendo del todo. Realiza algunas funciones interesantes.

El prompt es '#'. Escriba 'S' y recibirá (siempre) un informe de estado del sistema (corto/largo, según el uso del sistema), que contiene, entre otras cosas, el nombre del nodo del sistema. Si está activo, al escribir 'L' se mostrará un registro del sistema más completo. Esto es MUY útil. Contiene los nombres de usuario de los sistemas que llamaron al XMUX y los identificadores de usuario (UID), si se utilizan.

Como puedes ver, el XMUX parece bastante complicado a primera vista, pero en realidad es bastante simple. La forma más fácil de obtener el nombre del nodo es llamar al LOGGER.

El logger DEBE estar presente, siempre. Es un valor predeterminado que no se puede eliminar. El LCN se puede eliminar, pero el mnemónico debe permanecer.

Ya expliqué los mnemónicos anteriormente, pero te los refrescaré. Para usar el mnemónico, simplemente escribe el NUA, seguido de una coma y luego el mnemónico, por ejemplo:

12300456,LOGGER

Lo primero que ves en la cadena de datos es el nombre del nodo. Si es un espacio en blanco, te has encontrado con una rareza: un XMUX sin nombre de nodo.

El nombre del nodo es lo más común, aparte de las otras contraseñas comunes. Prueba combinaciones de este nombre y combinaciones de este con las palabras XMUX y MUX. Y por supuesto, si se usa un heraldo, utilice lo que encuentre en el heraldo.

Pero, de nuevo, si se trata de una empresa, les encanta usar el nombre o acrónimo de la empresa como contraseña, y ese acrónimo o nombre a menudo será el nombre del nodo.

¡Que lo disfrute!

Cuentas Comunes

```
Contraseñas de Consola
----------------
CONSOLE
XMUX
GANDALF
SYSTEM
PASSWORD
MUX
XMUX1
SYS
(nombre de nodo)
```

Una cosa más. No incluí el perfil ni los nombres de perfil remotos, ni los UID, ya que, hasta donde sé, no son aplicables desde el control remoto.

Y un último comentario. Los XMUX son potentes y potencialmente extremadamente dañinos para una red. NO BORRES NADA. Los únicos submenús a los que tendrás que acceder son 'DEFINE' y 'DISPLAY'. No expulses a la gente de los canales, ni añadas contraseñas de consola, ni elimines perfiles... acabarás en la cárcel. Derribar una red no tiene ninguna gracia para los administradores. Explora, no dañes.

STARMASTER

El Starmaster/PACx 2000 sigue siendo un sistema PACx algo misterioso, pero ya he explorado todas las barreras de seguridad, así como la red y las funciones internas, por lo que considero que esta información está bastante completa.

El sistema Starmaster/PACX es un sistema de red/servidor fabricado, de nuevo, por Gandalf Technologies Inc., Gandalf of Canada Ltd., en Canadá, y también se conoce informalmente (y de forma algo incorrecta) como el "Servidor de Acceso Gandalf". El Acceso es similar, pero diferente, como se describe más adelante. Es un sistema bastante popular en Datapac y se utiliza en otras regiones del mundo. De nuevo, se utiliza principalmente en redes de conmutación de paquetes, aunque - gracias al directorio de marcación de una salida Sam24V en un Starmaster - he descubierto que los Starmaster sí tienen acceso telefónico. La primera posible barrera de seguridad es la contraseña de acceso telefónico, que rara vez se usa, pero que conviene conocer.

El mensaje suele ser:

> DIALIN PASSWORD?

Se puede cambiar, aunque debería ser similar.

Las contraseñas de acceso telefónico tienen entre 1 y 8 caracteres y suelen ser una de las siguientes contraseñas predeterminadas:

> GANDALF SERVER PACX NET NETWORK STARMAST
> DIALIN PASSWORD ACCESS

Si el Starmaster tiene un XMUX residente (explicado en la definición del sistema anterior; XMUXs), averigüe el nombre del nodo e inténtelo.

La siguiente posible barrera de seguridad es que el administrador del sistema requiera que los usuarios introduzcan un nombre de usuario y una contraseña antes de acceder al servidor.

Aparecerá un mensaje como:

> USERNAME?

Este es el mensaje más común. Los nombres de usuario tienen entre 1 y 8 caracteres, y el Starmaster le indicará si son incorrectos o no con un mensaje de error como:

> INCORRECT USERNAME

o

> INVALID RESPONSE

Al igual que la solicitud de nombre de usuario, se puede cambiar, pero normalmente aparecerá en mayúsculas. Se permiten entre 1 y 10 intentos para un nombre de usuario o contraseña válidos, según la preferencia del propietario. Esto significa que (si se configura en diez intentos) puede ingresar 9 nombres de usuario inválidos, y en el décimo ingresar un nombre de usuario válido, y luego tener 10 intentos para una contraseña válida.

Los valores predeterminados para esta solicitud (que también enumeraré más adelante) son:

TEST, TESTUSER, TESTER, GANDALF, SYSTEM, GUEST USER, HP, CONSOLE OPERATOR.

Además, los nombres de pila suelen funcionar.

La siguiente solicitud que verá, o la primera si los nombres de usuario no están implementados, es la del servidor. Esta es la interfaz principal de usuario para un Starmaster; todos los comandos principales se utilizan desde aquí. Pero, como puedes imaginar, en realidad no se usan comandos, sino los nombres de los servicios.

A veces, al entrar en el servidor, verás una lista, pero otras veces solo tendrás que pulsar la línea de comandos del servidor, que suele tener un aspecto similar a:

SERVICE?

o

CLASS?

o incluso

service?

o

class?

o

service

O lo que el administrador del sistema considere oportuno. 'SERVICE?' es la opción

predeterminada y la más común. Ten en cuenta que los servicios PUEDEN tener contraseña, pero rara vez la tienen. En caso de tener contraseña, usa tu imaginación.

Otra cosa: en la consola PACx, donde se definen los servicios, existe una opción que decide si el servicio está permitido para usuarios remotos. Si está configurada en NO, entonces no podrás usarlo; tendrás que estar en una estación de trabajo para usar el comando. Esto es común en la CONSOLE y el MAIL, y ocasionalmente en módems y PADs. Recibirás un mensaje de error similar a 'SERVICE NOT ALLOWED'.

Proporcionaré una lista más completa de los servicios comunes, pero ahora mismo enumeraré los predeterminados y los principales.

- PAD, X25, X28 (o el nombre de tu PSN): Normalmente te llevarán a un PAD de Gandalf, cuyo prompt por defecto es *. 'HELP' mostrará una lista de comandos.

- MAIL: Una opción predeterminada que no se puede eliminar, pero nunca la he visto con la opción de acceso remoto en la posición ON.
- CONNECT: Otra opción predeterminada que no se puede eliminar y que nunca he visto con la opción de acceso remoto en la posición ON.
- MÓDEM, DIAL: Y sus variantes. El módem de salida más común es el Sam24V de Gandalf, que incluye un excelente conjunto de archivos de ayuda.
- CONSOLE: La herramienta principal. El controlador del sistema, el ordenador de mantenimiento, la máquina de pruebas y todo eso. NO confundas la consola PACX con la consola XMUX; son dos cosas muy diferentes. La consola debe ser protegida por el administrador del sistema con su vida, ya que cada facción del Starmaster se controla desde dentro de la Consola. CONSOLE es un servicio que no se puede eliminar del servidor, PERO el acceso remoto se puede eliminar, lo que nos impide acceder a ella. Inténtalo primero; si funciona, la pantalla se desplazará hacia abajo varias líneas y mostrará este mensaje:

  GANDALF TECHNOLOGIES INCORPORATED, COPYRIGHT 1990
  OPERATOR NAME?

Este nombre no se puede cambiar; permanecerá igual, salvo posiblemente la fecha de copyright.

Puede haber un máximo de 8 operadores, y tendrán entre 1 y 8 caracteres en su nombre y contraseña. Y de nuevo, el PACX te avisará si tu nombre de operador es incorrecto. Se te permitirán de 1 a 10 intentos con el nombre de usuario y luego se restablecerá a 0 para el intento de contraseña cuando encuentres un nombre de operador, pero el límite es el mismo.

Los mismos nombres de usuario predeterminados funcionan aquí, si tienes suerte, con la excepción de HP. Los listaré de nuevo al final.

Una vez dentro, todo está organizado en menús y es explicativo. NO LA CAGUES. Con eso me refiero a borrar o modificar. Mira. Hay MUCHO que ver. La consola PACX es increíblemente potente, y te divertirás mucho más explorándola. Además, una vez dentro de la consola, el juego ha terminado. Tienes el control de todos los servicios, usuarios y barreras de seguridad.

Si consigues una cuenta de consola de alto nivel, serás el dios de PACX, en serio.

Cuentas comunes

Usuarios	Contraseñas
CONSOLE	CONSOLE, PACX, GANDALF, OPERATOR, SYSTEM
GAND	GAND
GANDALF	GANDALF, SYSTEM, PACX, STARMAST, SYS
GUEST	GUEST, VISITOR, USER
HP	HP
OPERATOR	OPERATOR, SYSTEM, SYSLIB, LIB, GANDALF
SYSTEM	SYSTEM, SYS, OPERATOR, PACX, SYS, GANDALF
TEST	TEST, TESTUSER, USER, TESTER
TESTUSER	TEST, TESTUSER, USER, TESTER
TESTER	TEST, TESTUSER, USER, TESTER
USER	USER, GUEST, TEST, VISITOR, GANDALF

(nunca he visto una cuenta como MAINT, pero supongo que existe una, junto con los estándares por defecto del sistema. Prueba otras en relación con las anteriores).

```
Servicios
---------
1 (si funciona; más alto)
A (hasta la Z)
10 (si funciona; máyor en secuencia de decenas)
BBS
CLUSTER
CONNECT
CONSOLE
DATABASE
DATAPAC
DEC
DIAL
DIALOUT
FILES
FTP
GATEWAY
GEAC
HELP
HP
INTERNET
LIB
LIBRARY
LOOP
MAIL
MENU
MODEM
MUX
NET
NETWORK
OUT
OUTDIAL
PACX12
PACX24
PACX96
PAD
PRIME
PRIMOS
PROD
SALES
SERVER
SUN
SUNOS
SYS
SYSTEM
TELNET
TYMNET
UNIX
VAX
VMS
X25
X28
XCON
XGATE
XMUX
```

Y cualquier otra cosa que se te ocurra. Los nombres propios también son bastante comunes.

```
Nombre de Operador Contraseña
-----------------  --------
```

```
TEST            TEST, TESTUSER, USER, TESTER
TESTUSER        TEST, TESTUSER, USER, TESTER
TESTER          TEST, TESTUSER, USER, TESTER
GANDALF         GANDALF, SYSTEM, PACX, CONSOLE, SYS
GUEST           GUEST, VISITOR, USER
SYSTEM          SYSTEM, SYS, OPERATOR, PACX, SYS, GANDALF
                CONSOLE
USER            USER, GUEST, TEST, VISITOR, GANDALF
OPERATOR        OPERATOR, SYSTEM, CONSOLE, GANDALF
CONSOLE         CONSOLE, PACX, GANDALF, OPERATOR, SYSTEM
SYS             SYS, SYSTEM, GANDALF, PACX, CONSOLE
```

Y nuevamente, prueba nombres propios y CUALQUIER COSA de la que se te ocurra. Tu objetivo principal debe ser ingresar a la consola.

ACCESS2590:

El Access2590 es otra creación de Gandalf. Si bien es un sistema de servidor, difiere en algunos aspectos de un PACX.

El Starmaster generalmente solo conecta computadoras en una red local o de área amplia (se conecta a direcciones X.25 e IP, pero *normalmente* no lo hace), mientras que el Access 2590 se conecta a servicios de red local y de área amplia, direcciones X.25 y direcciones IP, con una sorprendente versatilidad. El PACX, sin embargo, tiene una distribución mucho más amplia.

Normalmente, mostrará una pantalla inicial de bienvenida, que a menudo le indicará que se trata de un servidor Access fabricado por Gandalf. Si el operador lo desea, puede incluir un menú de servicios con sus respectivas descripciones en este espacio. Luego, aparecerá un prompt, siendo el predeterminado: "Access 2590>". No he visto ningún tipo de protección inicial antes de que aparezca esa indicación, pero apuesto a que existe, y probablemente sea similar a la del PACX.

Sigue la tendencia que establecí con el PACX y no deberías tener problemas.

En fin, lo que más me gusta del Access 2590 en comparación con el Starmaster es el comando "show symbols". Ese era uno de los grandes problemas desde el punto de vista del hackeo con el PACX; no tiene un comando disponible para mostrar los servicios. Si obtienes acceso a la consola del PACX, puedes obtener una lista de servicios de esa manera, pero simplemente no puedes hackear una cuenta de consola cada vez, y además, a menudo el propietario habrá desactivado el acceso remoto a la consola.

Si el operador quería ayudarte con los servicios, tenía que tomar la iniciativa y diseñar una pantalla de aviso o implementar un servicio de ayuda, y pocos lo hacen. Pero la opción "Mostrar símbolos" en un Access te mostrará una lista de todos los "símbolos" disponibles, que es el término que usa Gandalf para referirse a los servicios. Conéctate a ellos con "c xxx", donde "xxx" es, por supuesto, el servicio.

Y sí, para aquellos entusiastas que ya han probado el poder de la consola PACX, el Access también tiene una consola. Escribe "c console" para acceder a ella. Sigue las instrucciones del PACX y todo irá bien.

PICK

El sistema PICK fue creado por Dick Pick (en serio), y es un sistema bastante extendido; existen varios en las principales PSN. Personalmente, no me gusta PICK, pero para aquellos que quieran probarlo, es un truco bastante sencillo.

Un mensaje de inicio de sesión PICK normal se ve así:

> 07 JUN 1993 04:00:21 Logon please:

Se pueden ingresar datos adicionales en esa línea y un encabezado que se puede usar encima. Sin embargo, los PICK suelen ser reconocibles por ese mensaje de inicio de sesión que normalmente contendrá la fecha y la hora, así como el mensaje "Logon please:". Si no estás seguro, ingresa el nombre de usuario "SYSPROG" en MAYÚSCULAS, ya que PICK distingue entre mayúsculas y minúsculas, y SYSPROG aparecerá en mayúsculas. SYSPROG es el superusuario (o, como lo llama PICK, el "Ultimate User") y es similar a root en Unix; debe estar presente.

PICK te avisa cuando has introducido un nombre de usuario no válido, lo cual es útil para encontrar cuentas válidas.

Puedes experimentar con mayúsculas y minúsculas si lo deseas, pero las mayúsculas son la norma.

Los creadores de PICK prefieren considerarlo más un sistema de gestión de bases de datos (DBMS) que un sistema operativo (SO), y a menudo se vende como tal. Por ello, puedes encontrarlo en sistemas basados en Unix, MPE y Primos, entre otros.

Una última nota: es posible el uso de contraseñas internas en PICK, así que no te sorprendas si crees haber encontrado un sistema sin contraseña y se te solicita una contraseña antes de la indicación interna.

Cuentas Comunes

Usernames	Passwords
1	
ACC	
ACCT	
ACCTNAME	
ACCUMATH	
ACCUPLOT	
ACCUPLOT-DEMO	ACCUPLOT, DEMO
ARCHIVE	
AUDITOR	
AUDITORS	
BACKUP	
BATCH	
BLOCK-CONVERT	
BLOCK-PRINT	
COLDSTART	
COMBINATION	
COMM	
COMTEST	
CPA	
CPA.DOC	CPA, DOC
CPA.PROD	CPA, PROD
CTRL.GROUP	CTRL, CONTROL
DEMO	
DA	

DCG	
DEV	
DM	DATA, MANAGER, MAN, MGR, DATAMGR, DATAMAN
DOS	
ERRMSG	
EXCEPTIONAL	
EXECUTE-CONTROL	
EXPRESS.BATCH	EXPRESS, BATCH
FILE-SAVE	FILESAVE, SAVE
FILE-TRANSFER	
FINANCE	
FLUSHER	
FMS	
FMS.PROD	FMS, PROD
GAMES	
GAMES.DOS	GAMES
GENERAL	
INSTANT	
INSTANT.DOS	INSTANT
JOB	
KILL	
LEARN	
LEARN.DLR	LEARN, DLR, LEARNDLR
LOGON	
LOTUS	
LOTUS.DOS	LOTUS
MAIL.BOX	MAIL
MINDER	
MODEM-SECURITY	
MOTD.DATA	MOTD
NETCOM	
NET.OFF	
NETOFF	
NETUSER	
NETWORK	
NEWAC	
NOLOG	
OLD.USER	
ON-LINE-DIAGS	DIAGS
PERFECT-BKGRND	
POINTER-FILE	
PRICE.DOS	PRICE
PRICES.DOS	PRICES
PROCLIB	PROC, LIBRARY, LIB
PROD	
PROMCOR	
PROMIS-ARCHIVE	PROMIS, ARCHIVE
PROMIS-BKGRND	PROMIS, BKGRND
PROMO	
PWP	
QA	QUALITY, CONTROL
SCC.SYSPROG	SCC, SYSPROG
SCREENLIB	
SECURITY	
SET.PLF	SET, PLF, PLFSET
SL	
SPSYM	
STUDENT	
SUPPORT	
SYM.DOS	SYM
SYS	
SYS.DOC	SYS
SYSLIB	SYSTEM, LIBRARY, SYS, LIB
SYSPROG	SYSTEM, PROGRAM, SYS, PROG, OPERATOR, DM

SYSPROG-PL	SYSPROG, PL
SYSTEM-ERRORS	
TCL	
TEMP	
TEMP-SYSPROG	TEMP, SYSPROG
TEST	
TEST-BKGRND	TEST
TRAINING	
TRY.DOS	TRY
ULTICALC	
ULTILINK	
ULTIMATION	
UNIMAX	
WORDS	
WP	
WP.DOS	WP
WP42.DOS	WP, WP42
WP50.DOS	WP, WP50
WP51	WP, WP51
WP51.DOS	WP, WP51
XES	

AOS/VS

AOS/VS es un sistema operativo de la Data General Corporation (DGC) y, en mi opinión, es el peor sistema operativo que he visto. Pero, en busca de conocimiento y para ampliar tus horizontes informáticos, te sugiero que intentes hackear incluso este sistema, por si te sirve de algo. AOS/VS suele identificarse fácilmente con un banner como este: (Sí, me estoy pasando de la raya, lo siento).

> **** AOS/VS Rev 7.62.00.00 / Press NEW-LINE to begin logging on ****
>
> AOS/VS 7.62.00.00 / EXEC-32 7.62.00.00 11-Jun-93 0:27:31 @VCON1
> Username:

La solicitud de nombre de usuario se parece engañosamente a un VMS, pero no lo es. Puedes comprobarlo introduciendo basura como nombre de usuario y contraseña. El AOS/VS responderá:

> Invalid username - password pair

El AOS/VS no te avisará si has introducido un nombre de usuario incorrecto. Un sistema estándar te permitirá cinco intentos con una combinación de nombre de usuario y contraseña, pero después mostrará este molesto mensaje:

> Too many attempts, console locking for 10 seconds

Que el sistema se bloquee durante 10 segundos no supone ningún problema para el hacker, salvo un pequeño intento de fuerza bruta (10 segundos). En cualquier caso, una vez dentro, al escribir "HELP" encontrarás una serie de archivos de ayuda, que no me resultaron muy útiles, y escribiendo "WHO" verás la lista de usuarios conectados.

Cuentas Comunes

Usuario	Password
guest	
op	operator, op
sysmgt	sys, mgt, system, man, mgr, manager

```
test
user
```

RSTS

Probablemente el sistema operativo más antiguo que aún existe sea RSTS. RSTS era un sistema operativo muy común hace una década, pero ahora está cerca de su extinción. Sin embargo, todavía quedan algunos en PSN, por lo que podrías intentar hackearlo.

El RSTS generalmente se identifica de la siguiente manera:

> RSTS V9.7-08 93.06.10 02:36
> User:

Antes de intentar hackear, prueba el comando SYSTAT. Es probable que esté deshabilitado, pero vale la pena intentarlo. RSTS te indicará si la ID que ingresaste es incorrecta con el mensaje de error:

> ?Invalid entry - try again

Los UID tienen el formato xxx,yyy, donde x e y son dígitos. Intenta adivinar UID hasta que encuentres uno con una contraseña. Además, los ID generalmente no superarán los 255 tanto en la posición x como en la posición y (es decir, 255,255 suele ser el ID más alto).

Cuentas Comunes

```
User ID    Password
-------    --------
1,2        SYSLIB
```

Windows NT

Realmente no sé mucho sobre Windows NT, principalmente porque se lanzó hace poco tiempo y no lo he visto en acción hasta la fecha. No sé cuándo se generalizará, pero para los futuros hackers, investigué un poco y encontré las dos cuentas predeterminadas del fabricante: "administrator" y "guest". Ambas vienen sin contraseña. Administrador es el equivalente a root en Unix, e invitado es justo lo que esperas: una cuenta de invitado de bajo nivel.

Curiosamente, en los manuales que vi, se animaba a los administradores de sistemas de WNT a mantener la cuenta de invitado... ¡sin contraseña! Muy gracioso... ¡veamos cuánto dura eso! En fin... Ah, sí... también distingue entre mayúsculas y minúsculas. Estoy bastante seguro de que es minúscula, pero es posible que la primera letra sea mayúscula.

Recuerda esto al intentar descifrar nuevas cuentas por fuerza bruta. Ah, y ten en cuenta posibles cuentas como "test" y "field" y similares.

Cuentas Comunes

```
Usuario
-------

administrator
guest
```

NETWARE

Novell Netware es el software de red local (LAN) para PC más común y es popular entre las escuelas secundarias. La seguridad interna (y externa, de hecho) es deficiente.

Cuentas Comunes

Usuario	Password
admin	operator, supervisor, sysadm
backup	
guest	visitor, user
netware	
novell	netware
public	
remote	
server	
staff	
supervisor	admin, operator, sysadm, supervis, manager
system1	
tape	backup
test	testuser
user	
visitor	guest

System75/85

Los sistemas System75/85 de AT&T han causado gran revuelo en los últimos meses, a pesar de llevar años en el mercado, principalmente debido a que algunos programadores descubrieron las funciones de la centralita.

En fin, la euforia ya pasó, así que probablemente sea seguro publicar la configuración predeterminada. Si no te gusta que haga esto, te aguantas. Cualquiera que tenga acceso a este archivo probablemente ya la tenga. Y si no, mejor aún. La información libre siempre ha sido uno de nuestros objetivos principales, y no pienso cambiar eso por culpa de unos pseudohackers inseguros.

Cuentas Comunes

Usuario	Password
browse	looker
craft	crftpw, craftpw
cust	custpw
field	support
inads	indspw, inadspw
init	initpw
rcust	rcustpw

AS400:

Otro sistema operativo que solo se usaba antes de mi época, AS-400. Es de IBM. Obtuve esta información de los antiguos mensajes de UPT, gracias a todos los que contribuyeron. Debería identificarse como un AS-400 al iniciar sesión.

No estoy seguro de si los caracteres distinguen entre mayúsculas y minúsculas... los escribiré en minúsculas, pero si no funciona, usaré mayúsculas.

Cuentas Comunes

```
Usuario
--------
qsecofr
qsysopr
quser
sedacm
sysopr
user
```

TSO

Un producto de IBM, puede encontrarse como una aplicación independiente, pero comúnmente se instala en un ISM. Al conectarse, verá una solicitud de inicio de sesión similar a esta:

> IKJ56700A ENTER USERID-

O algo parecido.

Le indicará si el nombre de usuario introducido es incorrecto:

> IKJ5642OI USERID xxx NOT AUTHORIZED TO USE TSO
> IKJ56429A REENTER-

En ocasiones, algunas cuentas tendrán el atributo STC y no se podrán usar para el inicio de sesión remoto.

Cuentas Comunes

```
Usuario     Password
--------    --------
admin       adm, sysadm, op
guest
init
maint
systest     test
test1       test
tso
```

Fuerza Bruta

Contraseñas

En ocasiones, te encontrarás en una situación en la que deseas penetrar en un sistema, pero las contraseñas predeterminadas están desactivadas y la ingeniería social no es posible.

Los hackers experimentados comienzan entonces con el tedioso proceso de probar contraseña tras contraseña, con la esperanza de forzar el acceso al sistema. Así nació el término "*Fuerza Bruta*", que describe acertadamente este proceso.

La fuerza bruta es la forma más agresiva de obtener una cuenta, pero suele ser efectiva. Es agresiva por varias razones relacionadas con el hecho de que - si la cuenta no se puede descifrar fácilmente - tendrás que llamar al sistema cientos de veces.

Primero explicaré, sin embargo, una manera diferente de fuerza bruta: la fuerza bruta *inteligente*. En este proceso, el hacker prueba el nombre del usuario (ya que es la contraseña más común), y una contraseña extraída de una base de datos de entre 20 y 100 contraseñas comunes. La diferencia con el ataque de fuerza bruta tradicional es que se reduce considerablemente el tiempo (pero también disminuyen las probabilidades de éxito).

Hoy en día, rara vez se realizan ataques de fuerza bruta *tradicional*; los grandes hackers de antaño dedicaban hasta 6 horas seguidas a probar contraseñas, pero hoy en día parece que con 5 minutos es suficiente. ¡Qué horror!

De realizarse un ataque de fuerza bruta *tradicional*, se lo suele automatizar. Esto significa que el hacker configura un programa o un script para generar un diccionario de contraseñas, y luego se va al cine o a hacer otra cosa. Obviamente, sea cual sea el método, el ataque de fuerza bruta *tradicional* es bastante peligroso. Un administrador de sistemas tendrá mayores probabilidades de darse cuenta que intentas 2000 veces introducir nombres de usuario y contraseñas que si lo haces 50 veces.

Si decides realizar un ataque de fuerza bruta *automatizado*, sería buena idea configurar un sistema ya hackeado para que lo haga por ti, por ejemplo un sistema Unix irrumpido. Sin embargo, no recomendaría desperdiciar la potencia de un Cray en una tarea tan insignificante como realizar ataques de fuerza bruta. Solo podrás ir tan rápido como te lo permita el sistema anfitrión. El peligro es evidente: tendrás que estar conectado al sistema remoto durante mucho tiempo, lo que te deja vulnerable a ser rastreado. La decisión es tuya.

Y, por supuesto, la fuerza bruta requiere un nombre de usuario. Si no tienes uno, probablemente no tengas suerte.

Algo que definitivamente deberías hacer es crear un listado de nombres de pila (que sea bastante completa). Puedes encontrar listados en medios en línea de tu país, o compra/roba un libro de nombres de bebé o revisa la guía telefónica y anota los nombres más comunes en un papel o en un fichero. Además de los nombres de pila propios, las contraseñas más comunes son los nombres de esposo/esposa, novio/novia y los nombres de los hijos, mascotas y equipos deportivos.

Bien, aquí están los fundamentos del hackeo inteligente por fuerza bruta:

1. Prueba el nombre de pila del usuario.

2. Prueba tu lista de nombres de pila, masculinos y femeninos.
3. Prueba el nombre de pila del usuario, con un dígito (del 1 al 9) después del nombre de usuario.
4. Prueba el nombre de pila del usuario, con una letra al final (de la A a la Z).
5. Prueba cualquier cosa relacionada con el sistema que estás usando. Si estás en un VAX con VMS en Datapac PSN, prueba VAX, VMS, Datapac, X25, etc.
6. Prueba cualquier cosa relacionada con la empresa o el servicio propietario del sistema. Si el usuario está en un sistema propiedad de Pepsi Cola, prueba con:
   Pepsi, Cola, Pepsico, etc.
7. Finalmente, prueba contraseñas de tu lista de contraseñas comunes. Tu lista de contraseñas comunes no debe tener más de 200 palabras.

Las contraseñas más populares son:

```
password secret money sex smoke beer x25 system hello cpu aaa abc fuck shit
```

Añade contraseñas populares según te parezca. Recuerda: la mayoría de las contraseñas se eligen espontáneamente, según lo que se le ocurra al usuario en ese momento (seguro que conoces esa sensación).

Intenta predecir la mente y el entorno del usuario, para pensar qué pensaría. Si no puedes, prueba con lo primero que se te ocurra, y lo irás descubriendo.

Ataque de fuerza bruta a nombres de usuario

Otra forma de ataque de fuerza bruta consiste en obtener un nombre de usuario para hackear contraseñas. Para adivinar un nombre de usuario válido, es necesario estar en un sistema que informe cuando el nombre de usuario no es válido; por lo tanto, VMS y Unix quedan descartados.

Existen dos tipos de nombres de usuario (según mi definición): de usuario y de sistema.

Los nombres de usuario de usuario son los nombres de usuario estándar. Algunos ejemplos serían: John, Smith, JMS, JSmith y JohnS.

Los nombres de usuario de sistema son nombres de usuario especiales utilizados por los operadores del sistema para realizar diversas funciones, como mantenimiento y pruebas. Dado que estos nombres de usuario (normalmente) no pertenecen a personas reales, se les asigna un nombre que corresponde a su función. Adivinar cualquiera de los dos tipos suele ser bastante fácil.

Los nombres de usuario de usuario suelen tener uno de dos formatos: Nombre o apellido. El formato más común es el nombre. Los formatos menos comunes son iniciales, inicial del nombre/apellido y nombre/inicial del apellido. En ocasiones, los formatos de nombre de usuario no tendrán nada que ver con nombres y, en su lugar, serán números de 6 u 8 dígitos. ¡Diviértete!

Los usuarios de un sistema casi siempre tendrán el mismo formato. Si adivinas uno, adivinar los demás no debería ser demasiado difícil. Para los nombres, consulta la lista que hiciste del libro de nombres de bebé. Para los apellidos, crea una lista de los apellidos más comunes, idealmente a partir de la guía telefónica, pero si te da pereza, tu mente servirá. SMITH y JONES son los apellidos no extranjeros más comunes. Para las iniciales, usa el sentido común. Intenta adivinar

combinaciones de 3 letras y usa formatos sensatos. Es decir, no uses XYZ como regla general; opta por JMS, PSJ, etc., para seguir la corriente de nombres y apellidos comunes. Si no tienes suerte, intenta cambiar las mayúsculas y minúsculas (es decir, de minúsculas a mayúsculas), ya que el sistema podría distinguir entre mayúsculas y minúsculas.

Normalmente no es necesario adivinar los nombres de los sistemas; he proporcionado un listado de los nombres predeterminados para los principales sistemas operativos. Pero si encuentras un sistema que no aparece en la lista, deberás descubrir sus propias configuraciones predeterminadas. Usa el sentido común y sigue las instrucciones con el nombre del nuevo sistema operativo y las utilidades que se ajusten a ese nombre. Intenta averiguar las restricciones de nombre de usuario para ese sistema; si los nombres de usuario deben tener 6 caracteres, prueba con nombres de usuario de solo 6 caracteres. Y, por último, aquí tienes una lista de configuraciones predeterminadas comunes (están en mayúsculas para mayor comodidad, pero por regla general se usan minúsculas).

```
OPERATOR SYSOP OP OPER MANAGER SYSMAN SYSMGR MGR MAN ADMIN
SYSADMIN ADM SYSADM BOSS MAIL SYSTEM SYS SYS1 MAINT SYSMAINT
TEST TESTER TESTUSER USER USR REMOTE PUB PUBLIC GUEST VISITOR
STUDENT DEMO TOUR NEWS HELP MGT SYSMGT SYSPROG PROD SALES
MARKET LIB LIBRARY FILES FILEMAN NET NETWORK NETMAN NETMGR
RJE DOS GAMES INFO SETUP STARTUP CONTROL CONFIG DIAG SYSDIAG
STAT SYSDIAGS DIAGS BATCH SUPRVISR SYSLIB MONITOR UTILITY
UTILS OFFICE CORP SUPPORT SERVICE FIELD CUST SECURITY WORD
DATABASE BACKUP FRIEND DEFAULT FINANCE ACCOUNT HOST ANON
SYSTEST FAX INIT INADS SETUP
```

Ataques de fuerza bruta a servicios

También está el momento en que te encuentras en un sistema de servidor y necesitas acceder a otros servicios. Seguramente se te notificará si el servicio que has ingresado es incorrecto, así que simplemente prueba con lo que se te ocurra, o recurre al siguiente listado de servicios (considera que muchas veces el servidor es capaz de distinguir entre el uso de mayúsculas y minúsculas; usa mayúsculas o minúsculas según prefieras):

(NOTA: Prueba también con dígitos (1+) y letras (A-Z)).

```
SERVER NETWORK NET LINK LAN WAN MAN CONNECT LOG LOGIN HELP DIAL
OUT OUTDIAL DIALOUT MODEM MODEMOUT INTERNET TELNET PAD X25 X28 FTP
SYSTEM SYS SYS1 SYSTEM1 UNIX VAX VMS HP CONSOLE INFO CMDS LIST
SERVICES SERVICE SERVICE1 COMP COMPUTER CPU CHANNEL CHANNEL1 CH1
CH01 GO DO ? LOG ID USERS SHOW WHO PORT1 PORT NODE1 NODE LINK1
DISPLAY CONFIG CONTROL DIAGS SYSDIAGS DIAG SYSDIAG HELLO EMAIL
MAIL SET DEFINE PARAMS PRINT PHONE PHONES SESSION SESSION1 BEGIN
INIT CUST SERVICE SUPPORT BUSINESS ACCT ACCOUNT FINANCE SALES
BUFFER QUEUE STAT STATS SYSINFO SYSTAT FTP ACCESS DISK LIB SYSLIB
LIBRARY FILES BBS LOOP TEST SEARCH MACRO CALL COMMANDS TYPE FIND
ASK QUERY JOIN ATTACH JOB REMOTE COM1 COM CALLER LOGGER MACHINE
BULLITEN CLUSTER RUN HELLO PAYROLL DEC
```

Ingeniería Social

Si bien no voy a profundizar en la ingeniería social (ES) en este momento, explicaré su premisa a quienes no estén familiarizados con ella.

La ingeniería social puede definirse de muchas maneras, pero mi definición se resume en: "Falsificación de la propia identidad verbalmente ante otra persona para obtener información que de otro modo sería inaccesible". Lo cual, en sí mismo, es una forma elegante de decir "manipulación, mentiras y, en general, engaños". La ingeniería social casi siempre se realiza por teléfono.

Les daré un ejemplo. Un hacker necesita información que no puede obtener mediante un simple hackeo (como el nombre de una cuenta). Llama telefónicamente a la empresa propietaria del sistema que desea infiltrar y dice ser Natalio Niceto de la filial local de Orletti Servicios Informáticos S.R.L, y que debe reparar sus computadoras o probarlas de forma remota. Pero, caramba, alguien del staff no anotó bien y no tiene cuenta. ¿Podría la amable señorita pasarle bien los datos para poder hacer el trabajo y contentar al jefe? ¿Entiendes la idea? Falsedad; fingir ser alguien que no eres. Si eres escéptico, no deberías serlo. El SEO es una técnica probada y eficaz, debido a que la mayor vulnerabilidad de seguridad de cualquier empresa son sus empleados. Una empresa puede diseñar un sistema con 20 contraseñas, pero si un empleado descuidado, sin darse cuenta, le proporciona todas esas contraseñas a un hacker, se acabó el juego.

Debes tener la voz adecuada. Si suenas como un niño de 12 años, no vas a conseguir nada. Si no puedes evitarlo, existen alteradores de voz para uso telefónico lo harán por ti (que todo profesional del SEO debería tener). Si la persona quiere contactar con una autoridad superior (que probablemente sospechará que algo anda mal), enfádate. No te enfurezcas, pero sí enójate. Explica que tienes un trabajo que hacer y sé persuasivo. No voy a profundizar más en SE, ya hay muchísimos archivos de texto sobre el tema. Recuerda mantener la calma, tener un plan B y es buena idea tener el guion escrito y practicarlo un poco antes. Si suenas natural y con autoridad, conseguirás lo que quieras. Y la práctica hace al maestro.

Registro de Residuos

El registro de residuos es otro tema que no abordaré en profundidad, pero ofreceré una breve descripción general.

El registro de residuos es el proceso de robar la basura de una empresa, rebuscar en ella y guardar la información valiosa. Se practica con mayor frecuencia en los distintos RBOC, pero si estás intentando hackear un sistema local, podría ser una buena idea registrar residuos durante algunas semanas; podrías encontrar un impreso o un trozo de papel con un nombre de usuario y contraseña de acceso telefónico.

Acrónimos

Esta es una lista básica de acrónimos de HP que he recopilado de diversas fuentes. Debería ser lo suficientemente extensa como para servir de referencia fácil sin resultar excesivamente engorrosa

ABSBH: Hora pico promedio en temporada alta

AC: Código de área

ACC: Control automático de comunicaciones

ACC: Centro de comunicaciones asíncronas

ACD: Distribuidor automático de llamadas

ACE: Equipo de llamada automática

ACF: Funciones avanzadas de comunicaciones

ACN: Código de área + Número

ADPCM: Modulación adaptativa por código de pulsos diferencial

AIS: Sistema de interceptación automática

ALFE: Interfaz de línea analógica

ALRU: Actualización automática de registro de línea

AM: Administrador de cuentas

AM: Módulo de acceso

AM: Modulación de amplitud

AMA: Contabilidad automática de mensajes

AMSAT: American Satellite

AN: Número asociado

ANI: Identificación automática de número

ANXUR: Analizador para redes con enrutamiento extendido

AOSS: Sistema de servicios de operador auxiliar

AP: Procesador adjunto

ARC: Control automático de respuesta

ARP: Protocolo de resolución de direcciones

ARPA: Agencia de proyectos de investigación avanzada

ARS: Sistema de respuesta automática

ARSB: Oficina de servicio de reparación automatizada

AT: Acceso tándem

ATB: Todas las troncales ocupadas

ATH: Notificación abreviada de problemas Historia

ATM: Cajero Automático

ATM: Modo de Transferencia Asíncrona

AT&T: American Telegraph and Telephone Company

AVD: Datos de Voz Alternativos

BCD: Decimal Codificado en Binario

BCUG: CUG Bilateral

BELLCORE: Bell Communications Research

BGP: Protocolo de Puerta de Enlace Fronteriza

BHC: Llamadas en Hora Ocupada

BLV: Verificación de Línea Ocupada

BOC: Bell Operating Company

BOR: Informe Básico de Salida

BOS: Supervisor de Oficina Comercial

BSC: Módulo Binario Síncrono

BSCM: Módulo de Comunicaciones Bisíncronas

BSOC: Bell Systems Operating Company

CA: Cable

CADV: Datos Alternativos/Voz Combinados

CAMA: Contabilidad Automática Centralizada de Mensajes

CATLAS: Sistema Centralizado Automático de Localización y Análisis de Problemas

CAU: Unidad de Acceso Controlado

CAVD: Voz Alternada/Datos Combinados

CBC: Encadenamiento de Bloques de Cifrado

CBS: Conmutación de Barra Cruzada

CBX: Centralita de Sucursal Computarizada

CBX: Centralita de Negocios Computarizada

CC: Tarjeta de Llamada

CC: Común Control

CC: Control Central

CC: Código de País

CCC: Complejo de Control Central

CCC: Capacidad de Canal Libre

CCC: Computadora de Control Central

CCIS: Señalización Interoficina de Canal Común

CCITT: Comité Consultivo Internacional de Telegrafía y Teléfono

CCM: Gestión de Control de Clientes

CCNC: Controlador de Red de Canal Común

CCNC: Centro de Redes de Comunicaciones Informáticas

CCS: Señalización de Canal Común

CCSA: Sistema de Conmutación de Control Común

CCSA: Sistema de Conmutación Central Común

CCSS: Sistema de Señalización de Canal Común

CCT: Terminal de Control Central

CCTAC: Centro de Análisis de Problemas de Comunicaciones Informáticas

CDA: Acumulador de Datos de Llamadas

CDA: Analizador de Volcado de Datos

CDA: Detección y Anuncio de Monedas

CDAR: Registro de Cuentas Marcadas por el Cliente

CDC: Corporación de Datos de Control

CDI: Identificación de Dígitos Circulares

CDO: Oficina de Marcación Comunitaria

CDPR: Receptor de Pulsos de Marcación del Cliente

CDR: Registro de Marcación de Llamadas

CDS: Sistema de Diseño de Circuitos

CEF: Instalación de Entrada de Cables

CERT: Equipo de Respuesta a Emergencias Informáticas

CF: Moneda Primero

CGN: Número de Grupo Concentrador

CI: Interconexión de Clúster

CIC: Códigos de Identificación de Operador

CICS: Sistema de Control de Información del Cliente

CID: Identificador de Llamada

CII: Índice de Identidad de Llamada

CIS: Servicio de Intercepción de Cliente

CISC: Computación de Conjunto de Instrucciones Complejas

CLASS: Servicio de Señalización de Área Local Personalizada

CLASS: Señalización Selectiva de Área Local Centralizada

CLDN: Número de Directorio de Línea Llamante

CLEI: Identificación de Equipo de Lenguaje Común

CLI: Identificación de Línea Llamante

CLID: Identificación de Línea Llamante

CLLI: Identificador de Ubicación de Lenguaje Común

CLNP: Protocolo de Red sin Conexión

CMAC: Centro Centralizado de Mantenimiento y Administración

CMC: Centro de Mantenimiento de Construcción

CMDF: Marco de Distribución Principal Combinado

CMDS: Sistema Centralizado de Datos de Mensajes

CMIP: Protocolo Común de Información de Gestión

CMS: Sistema de Gestión de Llamadas

CMS: Sistema de Monitoreo Conversacional

CMS: Sistema de Mantenimiento de Circuitos

CMS: Subsistema de Gestión de Comunicaciones

CN/A: Nombre/Dirección del Cliente

CNA: Aplicación de Red de Comunicaciones

CNAB: Oficina de Nombres y Direcciones de Clientes

CNCC: Cliente Centro de Control de Red

CNI: Interfaz de Red Común

CNS: Servicio de Red Complementario

CO: Oficina Central

COC: Código de Oficina Central

COCOT: Teléfono Operado con Monedas Propiedad del Cliente

CODCF: Instalación de Conexión de Datos de la Oficina Central

COE: Equipo de la Oficina Central

COEES: Sistema de Ingeniería de Equipo de la Oficina Central

COER: Informes de Equipo de la Oficina Central

COLT: Probador de Línea de la Oficina Central

COMSAT: Satélite de Comunicaciones

COMSEC: Seguridad de las Comunicaciones

COMSTAR: Sistema Común para Análisis e Informes Técnicos

CONS: Servicio de Red Orientado a la Conexión

CONTAC: Oficina Central Acceso a la red de oficina

COS: Clase de servicio

COSMIC: Interconexión principal de sistemas comunes

COR: Clase de restricción

COSMOS: Sistema computarizado para operaciones de mainframe

COT: Terminal de oficina central

CP: Programa de control

CPBXI: Interfaz de centralita privada computarizada

CPC: Centro de aprovisionamiento de circuitos

CPD: Distribuidor central de pulsos

CPMP: Plan de medición del rendimiento del operador

CRAS: Sistema administrativo de reparación de cables

CRC: Centro de registro de clientes

CRC: Centro de devoluciones de clientes

CREG: Extensión y ganancia de rango concentrada

CRG: Grupo de recursos centrales

CRIS: Sistema de información de registro de clientes

CRS: Sistema centralizado de resultados

CRSAB: Oficina centralizada de atención al cliente para reparaciones

CRT: Tubo de rayos catódicos

CRTC: Comisión Canadiense de Radio, Televisión y Telecomunicaciones

CSA: Área de servicio del operador

CSAR: Sistema centralizado de análisis e informes

CSC: Controlador de sitio celular

CSC: Centro de atención al cliente

CSDC: Capacidad digital de conmutación de circuitos

CSP: Moneda enviada y pagada

CSMA/CD: Múltiple de detección de operador Acceso/Detección de colisiones

CSR: Registros de Servicio al Cliente

CSS: Sistemas Especiales Informáticos

CSS: Subsistema Informático

CSU: Unidad de Servicio de Canal

CT: Transformador de Corriente

CTC: Cargo por Terminación de Canal

CTC: Centro Central de Pruebas

CTM: Módulo de Troncal de Contacto

CTMS: Sistema de Medición de Transmisión de Portadora

CTO: Transferencia de Llamadas Externas

CTSS: Sistema de Tiempo Compartido Compatible

CTSS: Sistema de Tiempo Compartido Cray

CTTN: Número de Ticket de Troncal de Cable

CTTY: Teletipo de Consola

CU: Unidad de Control

CU: Unidad de Cliente

CUG: Grupo de Usuarios Cerrados

CWC: Centrex de la Ciudad

DA: Información de Directorio

DACC: Finalización de Llamada de Asistencia de Directorio

DAA: Acuerdos de Acceso Digital

DACS: Sistema de Acceso Digital y Conexión Cruzada

DACS: Sistema de Cobro de Asistencia de Directorio

DAIS: Sistema de Intercepción Automática Distribuida

DAL: Línea de Acceso Dedicada

DAO: Operador de Asistencia de Directorio

DAP: Protocolo de Acceso a Datos

DARC: Centro de Registro de Alarmas de División

DARPA: Agencia de Proyectos de Investigación Avanzada del Departamento de Defensa

DARU: Unidad de Respuesta Automática Distribuida

DAS: Software de Acceso a Dispositivos

DAS: Sistema de Asistencia de Directorio

DAS: Distribuidor y Escáner

DAS: Estación de Doble Conexión

DASD: Dispositivo de Almacenamiento de Acceso Directo

DBA: Administrador de Bases de Datos

DBA: Arquitectura Empresarial Digital

DBAC: Centro de Administración de Bases de Datos

DBAS: Sistema de Administración de Bases de Datos

DBC: Centro Empresarial Digital

DBM: Gestor de Bases de Datos

DBMS: Sistema de Gestión de Bases de Datos

DBS: Selector de Bus Dúplex

DCA: Agencia de Comunicaciones de Defensa

DCC: Código de País de Datos

DCC: Ordenador de Recopilación de Datos

DCE: Equipo de Terminación de Circuito de Datos

DCE: Equipo de Comunicación de Datos

DCL: Lenguaje de Computadora Digital

DCLU: Unidad de Línea de Portadora Digital

DCM: Módulo de Portadora Digital

DCMS: Sistema de Medición de Llamadas Distribuidas

DCMU: Unidad de Medición de Concentrador Digital

DCO-CS: Conmutador Digital de Central Telefónica

DCP: Procesador Central Dúplex

DCS: Sistema de Interconexión Digital

DCSS: Segmentos Compartidos Discontinuos

DCSS: Servicios de Soporte Digital Personalizados

DCT: Portadora Digital Troncal

DDCMP: Protocolo de Mensajes de Comunicaciones de Datos Digitales

DDD: Marcación Directa a Distancia

DDN: Red de Datos de Defensa

DDR: Solicitud de Diseño de Datapac

DDS: Servicio de Datos Digitales

DDS: Sistema de Datos Digitales

DDS: Servicio Digital de Teléfonos de Datos

DEC: Corporación de Equipos Digitales

DES: Estándar de Cifrado de Datos

DF: Trama Distribuida

DGC: Corporación General de Datos

DH: Host Remoto

DID: Marcación Directa Entrante

DIMA: Arquitectura de Gestión de Información de Datos

DINS: Servicio de Red de Información Digital

DIS: Servicio de Información de Datapac

DISA: Acceso Directo al Sistema Entrante

DLC: Portadora de Bucle Digital

DLS: Servicio de Línea de Marcación

DM: Demultiplexor

DMA: Acceso Directo a Memoria

DN: Números de Directorio

DNA: Dirección de Red Datapac

DNA: Cuentas Digitales Nombradas

DNA: Arquitectura de Red Digital

DNIC: Código Identificador de Red de Datos

DNR: Registrador de Números Marcados

DNS: Servicio de Nombres de Dominio

DNS: Sistema de Nombres de Dominio

DOCS: Sistema de Consola del Operador de Visualización

DOD: Departamento de Defensa

DOM: Operaciones de Distrito Administrador

DPSA: Áreas de servicio de Datapac

DPTX: Ejecutivo de terminal de procesamiento distribuido

DSC: Compatibilidad de flujo de datos

DSI: Interfaz de abonado de datos

DSL: Línea de abonado digital

DSN: Red de servicios digitales

DSU: Unidad de servicio de datos

DSU: Unidad de servicio digital

DSX: Interconexión de señal digital

DTC: Controlador de troncales digitales

DTE: Equipo terminal de datos

DTF: Tono de marcado primero

DTG: Grupo de troncales directas

DTI: Interfaz de troncales digitales

DTIF: Formato de intercambio tabular digital

DTMF: Multifrecuencia de doble tono

DTN: Digital Red telefónica

DTST: Prueba de velocidad de tono de marcado

DVM: Multiplexor de voz y datos

EAEO: Central de acceso igualitario

EA-MF: Acceso igualitario multifrecuencia

EBDI: Intercambio electrónico de datos comerciales

EC: Operador de central telefónica

ECC: Cambio de cable

EDC: Centro de datos de ingeniería

EDI: Intercambio electrónico de datos

EE: Señalización de extremo a extremo

EEDP: Plan de marcación de conmutación electrónica en tándem ampliado

EGP: Protocolo de puerta de enlace exterior

EIES: Sistema de intercambio electrónico de información

EIU: Unidad de interfaz extendida

EKTS: Servicio telefónico electrónico de teclas

ELDS: Servicio de datos de línea de central telefónica

EMA: Arquitectura de gestión empresarial

EO: Central telefónica

EOTT: Troncalización de llamadas de la central telefónica

EREP: Grabación, edición e impresión ambiental

ESA: Sistema autónomo de emergencia

ESB: Oficina de servicios de emergencia

ESN: Número de serie electrónico

ESP: Proveedores de servicios mejorados

ESS: Sistema de conmutación electrónica

ESVN: Red de voz segura ejecutiva

ETS: Conmutación electrónica en tándem

EWS: Sistema de alerta temprana

FAC: Código de acceso a funciones

FAM: Administrador de Acceso a Archivos

FCC: Comisión Federal de Comunicaciones

FCO: Orden de Cambio de Campo

FDDI: Interfaz de Datos Distribuidos por Fibra

FDM: Multiplexación por División de Frecuencia

FDP: Programa de Desarrollo de Campo

FEP: Procesador Front-End

FEV: Voz de Extremo Remoto

FIFO: Primero en Entrar, Primero en Salir

FIPS: Estándar de Procedimiento de Información Federal

FM: Modulación de Frecuencia

FMAP: Proceso Automatizado de Fabricación de Campo

FMIC: Centro de Información de Fabricación de Campo

FOA: Aplicación de Primera Oficina

FOIMS: Sistema de Gestión de Información de Oficina de Campo

FPB: Bus de Paquetes Rápido

FRL: Nivel de Restricción de Instalaciones

FRS: Selección de Ruta Flexible

FRU: Unidad Reemplazable en Campo

FS: Servicio de Campo

FSK: Modulación por Desplazamiento de Frecuencia

FT: Prueba de Campo

FTG: Grupo de Troncales Finales

FTP: Protocolo de Transferencia de Archivos

FTPD: Demonio del Protocolo de Transferencia de Archivos

FX: Intercambio Exterior

GAB: Puente de Acceso de Grupo

GCS: Sistema de Control de Grupo

GECOS: Sistema Operativo Integral de General Electric

GGP: Protocolo de Puerta de Enlace a Puerta de Enlace

GOD: Salida Global Marcación

GPS: Sistema de Posicionamiento Global

GRINDER: Diseñador de Redes Interactivo Gráfico

GSA: Administración de Servicios Generales

GSB: Sistemas Generales de Negocios

GTE: Telefonía General

HCDS: Servicio Digital de Alta Capacidad

HDLC: Control de Enlace de Datos de Alto Nivel

HLI: Interconexión LAN de Alta Velocidad

HDSC: Portador de Señal de Alta Densidad

HPO: Opción de Alto Rendimiento

HUTG: Grupo de Troncales de Alto Uso

HZ: Hertz

IBM: Máquinas Comerciales Internacionales

IBN: Red Empresarial Integrada

IC: Portador Interurbano

IC: Portador InterLATA

IC: Portador de Intercambio

ICAN: Plan de Análisis de Circuito Individual

ICH: Gestión de Llamadas Internacionales

ICM: Gestión Integrada de Llamadas

ICMP: Protocolo de Mensajes de Control de Internet

ICN: Red de Interconexión

ICPOT: Portador de Intercambio - Punto de Terminación

ICUG: Grupo Internacional Cerrado de Usuarios

ICVT: Troncal de Verificación Entrante

IDA: Acceso Digital Integrado

IDCI: Interfaz Provisional Definida de Central Telefónica

IDDD: Marcación Directa Internacional de Distancia

IDLC: Portador de Bucle Digital Integrado

IDN: Digital Integrado Redes

IEC: Operador de Intercambio

IMP: Procesador de Mensajes de Internet

IMS: Sistemas de Gestión de la Información

IMS: Sistemas de Gestión Integrada

IMTS: Servicio Mejorado de Telefonía Móvil

INAP: Punto de Acceso Inteligente a la Red

INS: Sistema de Red de Información

INTT: Troncales Entrantes Sin Prueba

INWATS: Servicio de Telecomunicaciones de Área Amplia Entrante

IOC: Canal Interoficina

IOC: Controlador de Entrada/Salida

IOCC: Centro Internacional de Finalización en el Extranjero

IP: Punto Intermedio

IP: Protocolo de Internet

IPCF: Instalación de Comunicación Interprogramada

IPCH: Canal de Paginación Inicial

IPCS: Sistema Interactivo de Control de Problemas

IPL: Carga Inicial de Programa

IPLI: Interfaz de Línea Privada de Internet

IPLS: Servicios de Línea Privada InterLATA

IPSS: Servicio Internacional de Conmutación de Paquetes

IRC: Chat de Retransmisión de Internet

IRC: Operador Internacional de Registros

ISC: Centro de Conmutación Internacional

ISDN: Red Digital de Servicios Integrados

ISIS: Sistema de Información de Apoyo a la Investigación

ISO: Organización Internacional de Normalización

ISSN: Red Integrada de Servicios Especiales

ISU: Servicio Integrado Unidad

ISWS: Servicios de Software Internos

ITDM: Multiplexor Inteligente por División de Tiempo

ITI: Interfaz Interactiva de Terminal

ITS: Soporte Interactivo de Terminal

ITS: Sistema de Tiempo Compartido Incompatible

ITT: Telefonía y Telégrafo Internacional

IVP: Programa de Verificación de Instalación

IX: Ejecutivo Interactivo

IXC: Operador de Intercambio

JCL: Lenguaje de Control de Trabajos

JES: Sistema de Entrada de Trabajos

KP: Pulso de Tecla

LAC: Oficina de Asignación de Bucles

LADS: Área Local Servicio de datos

LADT: Transporte de datos de área local

LAM: Módulo de acceso de lóbulo

LAN: Red de área local

LAP: Protocolo de acceso de enlace

LAPB: Protocolo de acceso de enlace balanceado

LAPS: Procedimiento de acceso de enlace

LASS: Servicio de señalización de área local

LASS: Servicio de conmutación de área local

LAST: Transporte del sistema de área local

LAT: Transporte de área local

LATA: Área de transporte de acceso local

LAVC: Clúster VAX de área local

LBS: Sistema de balanceo de carga

LCDN: Número de directorio de última llamada

LCM: Módulo de concentración de línea

LCN: Canal lógico

LD: Larga distancia

LDEV: Dispositivo lógico

LDM: Módem de distancia limitada

LDS: Conmutador digital local

LEBC: Centro de negocios de gama baja

LEC: Operador de intercambio local

LEN: Redes de gama baja

LENCL: Clase de número de equipo de línea

LGC: Controlador de grupo de línea

LH: Host local

LIFO: Último en entrar, primero en salir

LIP: Protocolo de Internet grande

LLC: Control de enlace lógico

LM: Módulo de línea

LMOS: Sistema de mantenimiento y operaciones de bucle

LSI: Integración a gran escala

LTC: Controlador de línea troncal

LU: Uso local

LVM: Módulo de verificación de línea

MAC: Control de acceso al medio

MAC: Autenticación de mensajes

MAN: Red de área metropolitana

MAP: Puesto de mantenimiento y administración

MAP: Protocolo de automatización de fabricación

MAT: Línea troncal de acceso múltiple

MAU: Unidad de acceso multiestación

MBU: Unidad de negocio de fabricación

MCA: Arquitectura de microcanales

MCI: Microwave Communications, Inc.

MCP: Programa de control maestro

MCT: Tiempo de ciclo de fabricación

MCU: Unidad multichip

MDR: Registro de detalles de mensajes

MDS: Sistemas de diseño de mensajes

MDU: Unidad decodificadora de marcadores

MF: Multifrecuencia

MFD: Marco de distribución principal

MFR: Receptores multifrecuencia

MFT: Terminal de instalación metálica

MHZ: Megahercios

MIB: Base de información de gestión

MIC: Centro de información de gestión

MIF: Archivo maestro de artículos

MIS: Sistemas de información de gestión

MJU: Unidad de unión multipunto

MLHG: Grupo de búsqueda multilínea

MLT: Bucle mecanizado Pruebas

MNS: Base de la Red de Mensajes

MOP: Protocolo de Operación de Mantenimiento

MP: Multiprocesador

MPL: Línea Privada Multiprogramación

MPPD: Dispositivo Periférico Multiusos

MRAA: Acuerdo de Acceso a la Lectura de Medidores

MSCP: Protocolo de Control de Almacenamiento Masivo

MSI: Integración a Escala Media

MTBF: Tiempo Medio Entre Fallos

MTS: Servicio de Telecomunicaciones de Mensajes

MTS: Servicio de Telefonía de Mensajes

MTS: Servicio de Transporte de Mensajes

MTS: Servicio de Telefonía Móvil

MTSO: Oficina de Conmutación de Telecomunicaciones Móviles

MTU: Unidad de Terminación de Mantenimiento

MUX: Multiplexor

MVS: Almacenamiento Virtual Múltiple

MWI: Indicador de Mensaje en Espera

NAM: Módulo de Asignación de Números

NAS: Soporte de Aplicaciones de Red

NC: Canal de Red

NCCF: Instalación de Control de Comunicaciones de Red

NCI: Interfaz de Canal de Red

NCIC: Computadora Nacional de Información Criminal

NCP: Programa de Control de Red

NCS: Sistema de Computación de Red

NCTE: Equipo de Terminación de Canal de Red

NDA: Acceso a la Entrega de Red

NDC: Recopilación de Datos de Red

NDIS: Especificación de la interfaz del dispositivo de red

NDNC: Centro Nacional de Redes de Datos

NDS: Sistema de Datos de Red

NDU: Utilidad de Dispositivos de Red

NEBS: Sistema de Construcción de Equipos de Red

NECA: Asociación Nacional de Operadores de Intercambio

NFS: Compartición de Archivos de Red

NFS: Sistema de Archivos de Red

NFT: Transferencia de Archivos de Red

NI: Interconexión de Red

NI: Interfaz de Red

NIC: Centro de Información de Red

NIC: Tarjeta de Interfaz de Red

NJE: Entrada de Trabajo de Red

NLM: Módulos Cargables de Netware

NLM: Módulos Cargables de Red

NM: Módulo de Red

NMR: Rechazo de Modo Normal

NOS: Sistema Operativo de Red

NPA: Área del Plan de Numeración

NPA: Analizador de Rendimiento de Red

NSF: Fundación Nacional de Ciencias

NSP: Protocolo de Servicios de Red

NTE: Equipo Terminal de Red

NUA: Dirección de Usuario de Red

NUI: Identificador de Usuario de Red

OC: Centralización del Operador

OCC: Otro Operador Común

OD: Marcación Saliente

ODA: Arquitectura de Documentos de Oficina

ODDB: Base de Datos Dependiente de Oficina

ODI: Interfaz de Datos Abierta

OGT: Troncal Saliente

OGVT: Troncal de verificación saliente

OIS: Sistemas de información de oficina

OLTP: Procesamiento de transacciones en línea

ONI: Identificación del número de operador

OPCR: Programa de acciones del operador

OPM: Módulo de planta externa

OPM: Monitoreo del rendimiento de interrupciones

OR: Registro de origen

OS: Sistema operativo

OSI: Interconexión de sistemas abiertos

OSL: Localización de sistemas abiertos

OSS: Sistema de servicios del operador

OST: Tratamiento de la estación de origen

OTC: Compañía telefónica operadora

OTR: Informe de problemas operativos

OUTWATS: Servicio de telecomunicaciones de área amplia saliente

PABX: Centralita privada automatizada

PACT: Traductor de código de acceso de prefijo

PAD: Ensamblador/Desensamblador de paquetes

PADSX: Interconexión cruzada de señal digital parcialmente automatizada

PAM: Modulación de amplitud de pulso

PAX: Centralita privada automática

PBU: Unidad de negocio de producto

PBX: Centralita privada

PC: Centro primario

PCM: Modulación por código de pulso

PCP: PC Pursuit

PFM: Modulación por frecuencia de pulso

PGA: Matriz de rejilla de pines

PIN: Número de identificación personal

PLA: Matriz lógica programable

PLD: Dispositivo lógico programable

PLS: Secuenciador lógico programable

PM: Modulación de fase

PM: Módulo periférico

PMAC: Controlador de acceso de módulo periférico

PMR: Enrutamiento básico

PNC: Controlador de nodo Primenet

POC: Punto de contacto

POF: Instalación de operador programable

POP: Punto de presencia

POS: Punto de venta

POT: Punto de terminación

POTS: Servicio telefónico básico

PPN: Programa de proyecto Número

PPP: Protocolo Punto a Punto

PPS: Conmutación Pública de Paquetes

PPSN: Red Pública de Conmutación de Paquetes

PSAP: Centro de Atención de Llamadas de Seguridad Pública

PSDC: Capacidad Digital Conmutada Pública

PSDCN: Red de Comunicación de Datos Conmutados por Paquetes

PSDN: Red de Datos Conmutados por Paquetes

PSDS: Servicio Digital Conmutado Público

PSN: Red de Conmutación de Paquetes

PSS: Servicio de Conmutación de Paquetes

PSW: Palabra de Estado del Programa

PTE: Equipo de Transporte de Paquetes

PTS: Escáner de Posición y Troncales

PTT: Teléfono y Telégrafo Postal

PVC: Llamada Virtual Permanente

PVN: Red Virtual Privada

PWC: Centro de Cableado Primario

QPSK: Modulación por Desplazamiento de Fase en Cuadratura

RACF: Instalación de Control de Acceso a Recursos

RAO: Oficina de Contabilidad de Ingresos

RARP: Protocolo de Resolución de Direcciones Inversas

RBG: Grupo de Negocios en Tiempo Real

RBOC: Compañía Operadora Regional de Bell

RC: Centro de Tarifas

RC: Centro Regional

RDB: Base de Datos Relacional

RDSN: Región Digital Red conmutada

RDT: Transmisiones de datos restringidas

RDT: Terminal digital remoto

REP: Marcación repetitiva

REXX: Lenguaje de ejecución extendida reestructurada

RFC: Solicitud de comentarios

RIP: Protocolo de información de enrutamiento

RIS: Servicio de instalación remota

RISC: Computadora de conjunto de instrucciones reducido

RISD: Desarrollo de sistemas de información de referencia

RJE: Entrada remota de trabajos

RLCM: Módulo de concentración de línea remota

RNOC: Centro regional de operaciones de red

ROTL: Línea de prueba de oficina remota

RPC: Llamada a procedimiento remoto

RPE: Equipo periférico remoto

RSA: Arquitectura de sistema de referencia

RSB: Oficina de servicio de reparación

RSC: Centro de conmutación remota

RSCS: Subsistema de comunicaciones de cola remota

RSS: Sistema de conmutación remota

RSU: Unidad de conmutación remota

RTA: Arreglo de troncales remotas

RTG: Generador de enrutamiento

R/W: Lectura/Escritura

RX: Intercambio remoto

SA: Matriz de almacenamiento

SABB: Bloque de construcción de matriz de almacenamiento

SAM: Acceso seguro multipuerto

SARTS: Prueba remota de acceso conmutado Sistema

SAS: Servicios de Acceso Conmutado

SAS: Sistema de Conexión Única

SBB: Bloque de Construcción del Sistema

SABM: Modo Balanceado Asíncrono Establecido

SAC: Código de Área Especial

SBS: Sistemas de Negocios por Satélite

SC: Centro Seccional

SCC: Operador Común Especializado

SCC: Centro de Control de Conmutación

SCCP: Parte de Control de Conexión de Señalización

SCCS: Sistema del Centro de Control de Conmutación

SCF: Desvío Selectivo de Llamadas

SCF: Frecuencia de Control de Supervisión

SCM: Marca de Clase de Estación

SCM: Módulo de Portador

SCP: Punto de Conversión de Señal

SCP: Programa de Control del Sistema

SCP: Punto de Control de Servicio

SCR: Rechazo Selectivo de Llamadas

SDLC: Control de Enlace de Datos Síncrono

SF: Frecuencia Única

SFE: Front-End Seguro

SIDH: Inicio de Identificación del Sistema

SIT: Tonos de Información Especial

SLIC: Tarjeta de Interfaz de Línea de Abonado

SLIM: Módulo de Interfaz de Línea de Abonado

SLIP: Protocolo de Internet de Línea Serie

SLS: Sistema de Biblioteca de Almacenamiento

SLU: Unidad de Línea Serie

SM: Administrador del Sistema

SMDI: Almacenamiento Interconexión de disco de módulo

SMDR: Registro detallado del administrador de estación

SMI: Interrupción de administración del sistema

SMP: Multiprocesamiento simétrico

SMS: Servicios de automantenimiento

SMS: Sistema de administración de estación

SMTP: Protocolo simple de transferencia de correo

SNA: Arquitectura de red de sistemas

SNMP: Protocolo simple de administración de red

SONDS: Sistema de datos de red para pequeñas oficinas

SOST: Tratamiento de servicio de operador especial

SP: Procesador de servicio

SPC: Control de programa almacenado

SPCS: Sistema de control de programa almacenado

SPCSS: Sistema de conmutación de control de programa almacenado

SPM: Monitor de rendimiento de software

SQL/DS: Sistema de datos/lenguaje de consulta estructurado

SRC: Centro de recursos del sistema

SS: Sistema de señalización

SSAS: Sistema de señalización y anuncios de estación

SSCP: Punto de control de servicio de sistemas

SSCP: Punto de control de servicios de subsistema

SSP: Puntos de servicio de conmutación

SSS: Sistema de conmutación Strowger

ST: Inicio

STC: Cargo por Terminación de Servicio

STD: Marcación de Troncales de Abonado

STP: Punto de Transferencia de Señal

STS: Señal de Transporte Síncrona

SVC: Llamada Virtual Conmutada

SWG: Subgrupo de Trabajo

SxS: Conmutación Paso a Paso

T-1: Servicio Digital Terrestre

TAC: Código de Acceso a Troncales

TAC: Circuito de Acceso a Terminales

TAC: Centro de Acceso a Terminales

TAS: Servicio de Contestador Telefónico

TASI: Interpolación de Voz con Asignación de Tiempo

TBU: Unidad de Negocio de Terminales

TC: Centro de Llamadas

TCAP: Parte de Aplicación de Capacidades de Transacción

TCC: Centro de Consultoría Técnica

TCC: Computadora de Control de Telecomunicaciones

TCF: Instalación de Conexión Transparente

TCM: Multiplexación por Compresión de Tiempo

TCP: Protocolo de Control de Transmisión

TDAS: Sistema de Administración de Datos de Tráfico

TDCC: Comité de Coordinación de Datos de Transporte

TDM: Multiplexor por División de Tiempo

TDMS: Sistema de Gestión de Datos de Terminales

TDS: Servicio Digital Terrestre

TH: Historial de Problemas

TIDE: Distribuidor de Información de Tráfico Editor

TIS: Sistemas de Información Técnica

TLB: Puente TransLAN

TM: Módulo Troncal

TMSCP: Protocolo de Control de Almacenamiento Masivo en Cinta

TNDS: Sistema Total de Datos de Red

TNPS: Centro de Planificación de Redes de Tráfico

TO: Oficina de Peaje

TOP: Protocolo de Oficina Técnica

TOPS: Sistema de Posicionamiento del Operador de Tráfico

TP: Protocolo de Transporte

TP: Punto de Peaje

TP: Procesamiento de Transacciones

TPC: Consejo de Rendimiento del Procesamiento de Transacciones

TREAT: Herramienta de Evaluación y Análisis de Informes de Problemas

TRIB: Tasa de Rendimiento en Bits de Información

TRT: Radio y Telefonía Tropical

TSB: Entorno Básico de Tiempo Compartido

TSG: Generador de Señal de Sincronización

TSN: Red de Conmutación de Terminales

TSO: Opción de Tiempo Compartido

TSPS: Sistema de Posicionamiento del Servicio de Tráfico

TTL: Lógica Transistor a Transistor

TTS: Conmutador de Tiempo Troncal

TWX: Intercambio de Máquinas de Escribir

UA: Acuse de Recibo Sin Numerar

UAE: Error de Aplicación Irrecuperable

UART: Transmisor Receptor Asíncrono Universal

UCS: Estándar de Comunicación Uniforme

UDC: Universal Digital Canal

UDP: Protocolo de Datagramas de Usuario

UDVM: Multiplexor Universal de Voz y Datos

UID: Identificador de Usuario

UPC: Acondicionador de Puerto de Utilidad

USC: Recargo por Uso

USDN: Red Digital de los Estados Unidos

USTS: Sistemas de Transmisión de los Estados Unidos

UUCP: Programa de Copia de Unix a Unix

VAN: Redes de Valor Agregado

VAX: Extensión de Dirección Virtual

VCPI: Interfaz de Programa de Control Virtual

VDU: Unidad de Visualización

VF: Frecuencia de Voz

VFU: Unidad de Formularios Verticales

VFY: Verificar

VIA: Arquitectura de Información VAX

VLM: Módulo Virtual Cargable

VLSI: Integración a Muy Gran Escala

VMB: Buzón de Voz

VMCF: Instalación de Comunicaciones de Máquinas Virtuales

VMS: Sistema de Memoria Virtual

VMS: Sistema de Correo de Voz

VM/SP: Producto de Máquina/Sistema Virtual

VPA: Asesor de Rendimiento VAX

VPS: Sistema de Procesamiento de Voz

VSAM: Método de Acceso al Almacenamiento Virtual

VSE: Almacenamiento Virtual Extendido

VTAM: Método de Acceso a las Telecomunicaciones Virtuales

VTOC: Tabla de Contenidos de Volumen

VUIT: Visual Herramienta de interfaz de usuario

VUP: Unidad de procesamiento Vax

WAN: Red de área amplia

WATS: Sistema de telecomunicaciones de área amplia

WATS: Servicio telefónico de área amplia

WC: Centro de cableado

WCPC: Centro de planificación de cableado

WDCS: Sistema de interconexión digital de banda ancha

WDM: Multiplexación por división de longitud de onda

WES: Conmutación de Western Electronics

WUI: Western Union International

XB: Conmutación de barra cruzada

XBAR: Conmutación de barra cruzada

XBT: Conmutación en tándem de barra cruzada

XNS: Sistemas de red Xerox

XSV: Valor del sistema de costos de transferencia

XTC: Controlador de pruebas extendidas

Conclusión

Últimas palabras

Espero sinceramente que este archivo les haya sido útil y les animo a que lo distribuyan lo más ampliamente posible. Si les gustó, lo odiaron, tienen sugerencias o cualquier otra cosa, no duden en escribirme a mi dirección de internet (mi única dirección permanente por ahora) o a través de un BBS, si logran encontrarme.

Que se diviertan...

- Deicide -

Lecturas recomendadas

- *Neuromante*, *Mona Lisa Overdrive*, *Count Zero* y lo demás de William Gibson
- *The Hacker Crackdown*, de Bruce Sterling
- *Cyberpunk*, de Katie Hafner y John Markoff
- *The Cuckoo's Egg*, de Cliff Stoll

2600: El mejor fanzine impreso en papel.

($21 dólares estadounidenses, EE.UU. y Canadá.)

> Departamento de Suscripciones 2600,
> Apartado Postal 752, Middle Island,
> NY 11953-0752
> Teléfono: 516-751-2600 Fax: 516-751-2608

Los boletines electrónicos CUD, cDc y Phrack, así como los TJ de LOD/H, se pueden encontrar en internet y en cualquier foro de radioaficionados de calidad.

BBS

Aunque la mayoría de los BBS tienen una vida útil tan corta como la de una mosca de la fruta, por fin tengo una lista relativamente estable. Entrar en ellos es tu problema. Solo sé tú mismo y ten ganas de aprender.

- Unphamiliar Territories
- Demon Roach Underground
- Temple of the Screaming Electron
- Burn This Flag
- Dark Side of the Moon
- ...y Phrozen Realm si regresa.

Referencias

Todo el material utilizado en esta publicación es original, a menos que se indique lo contrario.

Sin embargo, quiero agradecer a Phrack y a LOD/H por sus archivos de texto, que me dieron un valioso impulso en la dirección correcta.

Y, por supuesto, a toda la gente maravillosa de h/p que me ha ayudado en el camino.

Y finalmente:

Gracias a la EFF por su continuo apoyo a todos los derechos del mundo, en esta era tecnológica.

Gracias a todos los que gestionan las FreeNets y que siguen apoyando el derecho al libre acceso a la información en este mundo de cinismo.

Gracias a cDc por no haberse vendido después de tantos años...

Inspiraciones musicales: Primus, Rage Against the Machine, Jimi Hendrix, Led Zeppelin, Dead Kennedys, White Zombie, Beastie Boys, etc., etc.

> "Yes I know my enemies. They're the teachers who taught me to fight me. Compromise, conformity, assimilation, submission, ignorance, hypocrisy, brutality, the elite"
>
> - /Know Your Enemy/ (c) Rage Against the Machine

- Deicide -
deicide@west.darkside.com

Aviso Legal

Este archivo se proporciona únicamente con fines informativos.

El autor no se responsabiliza de las acciones de ninguna persona tras leer este archivo.